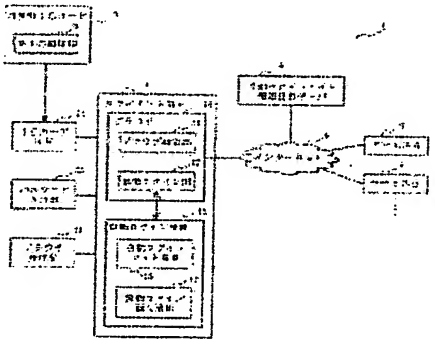
PTU 030005

AUTOMATIC LOG-IN SYSTEM, AUTOMATIC LOG-IN METHOD, AUTOMATIC LOG-IN PROGRAM, AND STORAGE MEDIUM

Publication number: JP2004151863 (A)
Publication date: 2004-05-27
Inventor(s): KATO TAKATOSHI; WAKASA SHIGEKI; NAKAYAMA HIROSHI; NAGASHIMA ATSUSHI +
Applicant(s): SONY CORP +
Classification:
- International: ***G06F13/00; G06F15/00; G06F21/20; G09C1/00; H04L9/32;*** **G06F13/00; G06F15/00; G06F21/20; G09C1/00; H04L9/32;** (IPC1-7): G06F13/00; G06F15/00; G09C1/00; H04L9/32
- European:
Application number: JP20020314680 20021029
Priority number(s): JP20020314680 20021029

Abstract of **JP 2004151863 (A)**

PROBLEM TO BE SOLVED: To provide an automatic log-in system having high safety in terms of security, and reducing the load of any log-in operation to each site. ; SOLUTION: A browser 10 is provided with a browser functioning part 11 for exhibiting a browser function and an automatic log-in part 12 for automatically logging-in a service site. Automatic log-in information 15 is configured of automatic log-in site information 16 which can be decoded with first key information 9 acquired from a non-contact IC card 7 and automatic log-in personal information 17 which can be multiplexed with the first key information 9 and an automatic log-in password. When the browser functioning part 11 performs access to a log-in page registered with the automatic log-in information 15, the automatic log-in part 12 generates a log-in request by using the automatic log-in information 15, and transmits it to a server 5. ; COPYRIGHT: (C)2004,JPO



PTH030008

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-151863
(P2004-151863A)
(43)公開日　平成16年5月27日(2004.5.27)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	330B	5B085
G06F 13/00	G06F	15/00	330G	5J104
G09C 1/00	G06F	13/00	510S	
H04L 9/32	G09C	1/00	640E	
	H04L	9/00	673A	

審査請求 未請求　請求項の数 31　OL　（全 36 頁）　最終頁に続く

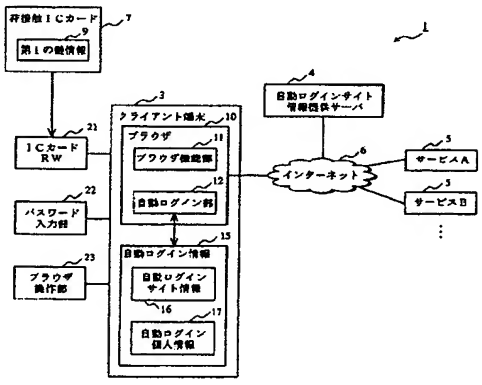
(21)出願番号　特願2002-314680(P2002-314680)
(22)出願日　平成14年10月29日(2002.10.29)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100096655
弁理士　川井　隆
(74)代理人　100091225
弁理士　仲野　均
(72)発明者　加藤　孝俊
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　若狭　繁基
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】自動ログインシステム、自動ログイン方法、自動ログインプログラム、及び記憶媒体

(57)【要約】
【課題】セキュリティ面で安全性が高く、各サイトへのログイン操作の負担を軽減することができる自動ログインシステムなどを提供すること。
【解決手段】ブラウザ１０は、ブラウザ機能を発揮するブラウザ機能部１１と、サービスサイトに自動的にログインする自動ログイン部１２を備えている。自動ログイン情報１５は、非接触ＩＣカード７から取得した第１の鍵情報９で復号化できる自動ログインサイト情報１６と、第１の鍵情報９と自動ログインパスワードで複合化できる自動ログイン個人情報１７から構成されている。自動ログイン部１２は、ブラウザ機能部１１が自動ログイン情報１５で登録してあるログインページにアクセスすると、自動ログイン情報１５を用いてログインリクエストを生成し、サーバ５に送信する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする自動ログイン装置を備えた自動ログインシステムであって、
前記自動ログイン装置は、
鍵情報を記憶したＩＣカードから前記鍵情報を取得する鍵情報取得手段と、
自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて復号化する復号化手段と、
前記復号化した自動ログイン情報を用いて前記サービスサイトに自動ログインする自動ログイン手段と、
を具備したことを特徴とする自動ログインシステム。
【請求項２】
前記自動ログイン情報の少なくとも一部を前記自動ログイン装置に提供する自動ログイン情報提供サーバを備えたことを特徴とする請求項１に記載の自動ログインシステム。
【請求項３】
前記ＩＣカードは、非接触型ＩＣカードであることを特徴とする請求項１に記載の自動ログインシステム。
【請求項４】
前記自動ログイン装置は、
前記自動ログイン情報記憶手段を具備したことを特徴とする請求項１に記載の自動ログインシステム。
【請求項５】
前記ＩＣカードは、前記自動ログイン情報の少なくとも一部を記憶しており、前記自動ログイン装置は、前記ＩＣカードから前記自動ログイン情報の少なくとも一部を取得することを特徴とする請求項１に記載の自動ログインシステム。
【請求項６】
前記自動ログイン情報は、サービスサイト毎に構成されており、
前記自動ログイン装置は、
ユーザがサービスサイトを選択するサイト選択手段と、
前記選択したサービスサイトに対する前記自動ログイン情報を検索する自動ログイン情報検索手段と、
を具備し、
前記自動ログイン手段は、前記検索した自動ログイン情報を用いて前記サービスサイトに自動ログインすることを特徴とする請求項１に記載の自動ログインシステム。
【請求項７】
前記自動ログイン情報は、
自動ログイン対象のサービスサイトを特定するサービスサイト特定情報と、前記サービスサイト特定情報で特定される前記サービスサイトへのログイン処理を前記サービス提供サーバに要求するログインリクエスト情報と、を有する自動ログインサイト情報と、
前記サービス提供サーバがユーザを認証するのに要するユーザ認証情報を有する自動ログイン個人情報と、
から構成されていることを特徴とする請求項１に記載の自動ログインシステム。
【請求項８】
前記自動ログイン装置は、第２の鍵情報を取得する第２の鍵情報取得手段を具備し、
前記自動ログイン個人情報は、前記ＩＣカードから取得した鍵情報と、前記取得した第２の鍵情報を用いて復号化可能に暗号化されており、
前記復号化手段は、前記鍵情報と前記第２の鍵情報を用いて前記自動ログイン個人情報復号化することを特徴とする請求項７に記載の自動ログインシステム。
【請求項９】

前記自動ログインサイト情報と、前記自動ログイン個人情報は、サービスサイト毎に対応付けられて構成されており、
前記自動ログイン装置は、
ユーザがサービスサイトを選択するサイト選択手段と、
前記選択したサービスサイトに対する前記自動ログインサイト情報を検索する自動ログインサイト情報検索手段と、
前記検索した自動ログインサイト情報に対応付けられた自動ログイン個人情報を検索する自動ログイン個人情報検索手段と、
前記検索した自動ログインサイト情報に含まれるログインリクエスト情報と前記検索した自動ログイン個人情報に含まれるユーザ認証情報とを用いてサービス提供サーバがログイン処理を行うのに用いるログインリクエストを生成するログインリクエスト生成手段と、
を具備し、
前記自動ログイン手段は、前記生成したログインリクエストを前記選択したサービスサイトが設けられたサービス提供サーバに送信することを特徴とする請求項７に記載の自動ログインシステム。

【請求項１０】
前記自動ログイン装置は、
前記検索された前記自動ログインサイト情報に対応する前記自動ログイン個人情報が検索できなかった場合、ユーザから入力される情報を用いて前記自動ログインサイト情報に対応する自動ログイン個人情報を、前記第１の鍵情報と前記第２の鍵情報で復号化可能に暗号化して追加する自動ログイン個人情報追加手段を具備したことを特徴とする請求項８に記載の自動ログインシステム。

【請求項１１】
前記自動ログイン装置が、
前記自動ログイン情報を記憶する自動ログイン情報記憶手段を具備したことを特徴とする請求項７に記載の自動ログインシステム。

【請求項１２】
前記自動ログイン情報記憶手段は、前記自動ログイン装置に着脱可能な記憶媒体に前記自動ログイン個人情報を記憶することを特徴とする請求項１１に記載の自動ログインシステム。

【請求項１３】
請求項１０に記載の自動ログインサイト情報を前記自動ログイン装置に送信する自動ログインサイト情報提供サーバを備えたことを特徴とする請求項１０に記載の自動ログインシステム。

【請求項１４】
前記自動ログイン装置は、
前記ＩＣカードが前記自動ログイン装置にセットされているか否かを検出する検出手段と、
前記検出手段で前記ＩＣカードがセットされていないと検出した場合に、前記自動ログイン装置に対する入力をロックするロック機構と、
を具備したことを特徴とする請求項１に記載の自動ログインシステム。

【請求項１５】
請求項１２に記載の記憶媒体であって、自動ログイン個人情報を記憶し、前記クライアント端末に着脱可能な記憶媒体。

【請求項１６】
サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする自動ログイン装置を用いた自動ログイン方法であって、
前記自動ログイン装置は、鍵情報取得手段と、復号化手段と、自動ログイン手段と、を備え、

前記鍵情報取得手段で、鍵情報を記憶したＩＣカードから前記鍵情報を取得する鍵情報取得ステップと、
自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて前記復号化手段で復号化する復号化ステップと、
前記復号化した自動ログイン情報を用いて、前記自動ログイン手段で、前記サービスサイトに自動ログインする自動ログインステップと、
から構成されたことを特徴とする自動ログイン方法。
【請求項１７】
自動ログイン情報提供サーバが、前記自動ログイン情報の少なくとも一部を前記自動ログイン装置に提供する自動ログイン情報提供ステップを備えたことを特徴とする請求項１６に記載の自動ログイン方法。
【請求項１８】
前記ＩＣカードは、非接触型ＩＣカードであることを特徴とする請求項１６に記載の自動ログイン方法。
【請求項１９】
前記自動ログイン装置は、前記自動ログイン情報記憶手段を具備し、
前記自動ログイン情報記憶手段から、前記自動ログイン情報を取得する自動ログイン情報取得ステップを備えたことを特徴とする請求項１６に記載の自動ログイン方法。
【請求項２０】
前記ＩＣカードは、前記自動ログイン情報の少なくとも一部を記憶しており、前記ＩＣカードから前記自動ログイン情報の少なくとも一部を取得する取得ステップを備えたことを特徴とする請求項１６に記載の自動ログイン方法。
【請求項２１】
前記自動ログイン情報は、サービスサイト毎に構成されており、
前記自動ログイン装置は、サイト選択手段と、自動ログイン情報検索手段と、
を備え、
前記サイト選択手段で、ユーザがサービスサイトを選択するサイト選択ステップと、
前記選択したサービスサイトに対する前記自動ログイン情報を、前記自動ログイン情報検索手段で検索する自動ログイン情報検索ステップと、
を備え、
前記自動ログインステップでは、前記検索した自動ログイン情報を用いて前記サービスサイトに自動ログインすることを特徴とする請求項１６に記載の自動ログイン方法。
【請求項２２】
前記自動ログイン情報は、
自動ログイン対象のサービスサイトを特定するサービスサイト特定情報と、前記サービスサイト特定情報で特定される前記サービスサイトへのログイン処理を前記サービス提供サーバに要求するログインリクエスト情報と、を有する自動ログインサイト情報と、
前記サービス提供サーバがユーザを認証するのに要するユーザ認証情報を有する自動ログイン個人情報と、
から構成されていることを特徴とする請求項１６に記載の自動ログイン方法。
【請求項２３】
前記自動ログイン装置は、第２の鍵情報取得手段を具備し、
前記第２の鍵情報取得手段で、第２の鍵情報を取得する第２の鍵情報取得ステップを備え、
前記復号化ステップで、前記自動ログイン個人情報を、前記ＩＣカードから取得した鍵情報と、前記取得した第２の鍵情報を用いて復号化することを特徴とする請求項２２に記載の自動ログイン方法。
【請求項２４】
前記自動ログインサイト情報と、前記自動ログイン個人情報は、サービスサイト毎に対応付けられて構成されており、

前記自動ログイン装置は、サイト選択手段と、自動ログインサイト情報検索手段と、自動ログイン個人情報検索手段と、ログインリクエスト生成手段と、を具備し、
前記サイト選択手段で、ユーザがサービスサイトを選択するサイト選択ステップと、
前記自動ログインサイト情報検索手段で、前記選択したサービスサイトに対する前記自動ログインサイト情報を検索する自動ログインサイト情報検索ステップと、
前記検索した自動ログインサイト情報に対応付けられた自動ログイン個人情報を、前記自動ログイン個人情報検索手段で検索する自動ログイン個人情報検索ステップと、
前記検索した自動ログインサイト情報に含まれるログインリクエスト情報と前記検索した自動ログイン個人情報に含まれるユーザ認証情報とを用いてサービス提供サーバがログイン処理を行うのに用いるログインリクエストを前記ログインリクエスト生成手段で生成するログインリクエスト生成素ステップと、
前記生成したログインリクエストを前記選択したサービスサイトが設けられたサービス提供サーバに送信する送信ステップと、
を備えたことを特徴とする請求項２２に記載の自動ログイン方法。
【請求項２５】
前記自動ログイン装置は、自動ログイン個人情報追加手段を具備し、
前記検索された前記自動ログインサイト情報に対応する前記自動ログイン個人情報が検索できなかった場合、ユーザから入力される情報を用いて前記自動ログインサイト情報に対応する自動ログイン個人情報を、前記自動ログイン個人情報追加手段で、前記第１の鍵情報と前記第２の鍵情報で復号化可能に暗号化して追加する自動ログイン個人情報追加ステップを具備したことを特徴とする請求項２３に記載の自動ログイン方法。
【請求項２６】
前記自動ログイン装置が、
前記自動ログイン情報を記憶する自動ログイン情報記憶手段を具備し、
前記自動ログイン情報記憶手段から、前記自動ログイン情報を取得する自動ログイン情報取得ステップを備えたことを特徴とする請求項２２に記載の自動ログイン方法。
【請求項２７】
前記自動ログイン情報取得ステップでは、前記自動ログイン装置に着脱可能な記憶媒体から前記自動ログイン個人情報を取得することを特徴とする請求項２６に記載の自動ログイン方法。
【請求項２８】
自動ログインサイト情報提供サーバから、請求項２５に記載の自動ログインサイト情報を前記自動ログイン装置に送信する自動ログインサイト情報送信ステップを備えたことを特徴とする請求項２５に記載の自動ログイン方法。
【請求項２９】
前記自動ログイン装置は、検出手段と、ロック機構とを具備し、
前記検出手段で、前記ＩＣカードが前記自動ログイン装置にセットされているか否かを検出する検出ステップと、
前記検出手段で前記ＩＣカードがセットされていないと検出した場合に、前記ロック機構で、前記自動ログイン装置に対する入力をロックするロックステップと、
を備えたことを特徴とする請求項１６に記載の自動ログイン方法。
【請求項３０】
サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする機能をコンピュータに発揮させるための自動ログインプログラムであって、
鍵情報を記憶したＩＣカードから前記鍵情報を取得する鍵情報取得機能と、
自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて復号化する復号化機能と、
前記復号化した自動ログイン情報を用いて前記サービスサイトに自動ログインする自動ログイン機能と、

をコンピュータで実現するための自動ログインプログラム。
【請求項３１】
サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする機能をコンピュータに発揮させるための自動ログインプログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、
鍵情報を記憶したＩＣカードから前記鍵情報を取得する鍵情報取得機能と、
自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて復号化する復号化機能と、
前記復号化した自動ログイン情報を用いて前記サービスサイトに自動ログインする自動ログイン機能と、
をコンピュータで実現するための自動ログインプログラムを記憶したコンピュータが読み取り可能な記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、自動ログインシステムなどに関し、特に、ＩＣカードに記憶されている鍵情報を用いて、ログインに必要な情報を復号化し、これを用いてサービスサイトに自動ログインするものに関する。
【０００２】
【従来の技術】
近年の急速なインターネットの普及により、誰でもインターネットを介して様々なサービスを享受することができるようになってきた。
また、インターネット上で提供されるサービスも、ニュース、天気予報、テレビ番組表、広告など、ユーザに情報を提供するものの他、銀行預金の管理、有価証券の売買などユーザの資産を管理するものまで多岐に渡っている。
これら、インターネット上でサービスを提供するサービスサイトには、ユーザが入力したログインＩＤやパスワードなどからユーザを認証するものがある。
このようなサービスサイトにアクセスする際、ユーザは、当該サービスサイトに設定してあるログインＩＤやパスワードをキーボードなどの入力装置を用いて入力する。
このようにして、ユーザを認証することにより、ユーザに固有のサービスを提供したり、システムのセキュリティを高めたりしている。
【０００３】
図１７は、従来のログイン方法を説明するための図である。
クライアント端末１００１は、インターネット１００２を介してサービスＡを提供するサーバ１００５とサービスＢを提供するサーバ１００６に接続可能に配設されている。ここで、サービスサイトＡ、Ｂにログインするために、ログインＩＤとパスワードを入力するものとする。
この場合、クライアント端末１００１からサーバ１００２にアクセスしてサーバ１００２が提供するサービスＡを利用するためには、サービスＡを提供するログインページ（例えば、「ｈｔｔＰ：／／ｗｗｗ．ｓｅｒｖｅｒＡ．ｃｏｍ／ｓｅｒｖｉｃｅＡ／ｌｏｇｉｎ．ｈｔｍｌ」などのＵＲＬで特定される）にアクセスし、ログインＩＤとパスワードをキーボードから入力する。
【０００４】
また、クライアント端末１００１から、サーバＢが提供するサービスＢを利用するためには、サービスＢのログインページ（例えば、「ｈｔｔＰ：／／ｗｗｗ．ｓｅｒｖｅｒＢ．ｃｏｍ／ｓｅｒｖｉｃｅＢ／ｌｏｇｉｎ．ｈｔｍｌ」などのＵＲＬで特定される）にアクセスし、ログインＩＤとパスワードを入力する。
なお、通常はログインに使用するログインＩＤとパスワードは、サイト毎に異なっており、インターネット上の各サイトにログインする場合、ユーザは、キーボードなどを用いて

、その都度、当該サイト用のログインＩＤとパスワードを入力する必要がある。
このような、キーボードからのログインＩＤ及びパスワードの入力の煩わしさを改善し、キーボードよりログインＩＤとパスワードの入力を行わずに目的のサイトにログインする技術として次のものがある。
【０００５】
【特許文献１】特開２００２－１７５２８１号公報
【特許文献２】特開２００２－４１３８０号公報
【０００６】
上記特許文献１の「ネットワークログインシステム」は、パーソナルコンピュータとＩＣカード内蔵の携帯端末から暗証番号を入力して、ネットワーク上のサイトへの自動ログインを行う技術である。ＩＣカードにはネットワーク接続権限の有無や、ログイン時の暗証番号が記録されており、入力された暗証番号の認証を経て、ネットワークへの接続が許可される。
また、上記特許文献２の「データ処理システム及び方法」は、クライアント端末側でサーバ側が提供するインターネットサービスへのログインリクエストをブックマークとして管理しておき、これを用いて認証処理を省いて自動ログインを行うものである。より詳細には、このブックマークには、認証を受けるサイトへのログインＩＤ、及びパスワードを暗号化した情報を含むサイトＵＲＬが登録されており、当該ブックマークから登録されたＵＲＬを選択することで、認証サイトはログイン情報を抽出して認証を行う。
【０００７】
【発明が解決しようとする課題】
ところが、上記特許文献１の技術は、ある特定のシステムへのログイン方法を提供しており、インターネット上の複数サイトのサーバへの（個々のサービスでログインＩＤとパスワードが異なる）ログインを自動で行う汎用的な仕組みではないという問題があった。また、ＩＣカード内認証を経て、認証結果のみがネットワークへ送信されるものであり、認証を必要とする複数サイトへの自動ログインするものではない。
また、上記特許文献２の技術は、クライアント端末が第三者の手に渡った場合に、セキュリティの面から問題があった。即ち、ブックマークを登録しているクライアント端末を自由に他人が使える環境にある場合、誰もが自動ログインできてしまう。
【０００８】
そこで、本発明の目的は、セキュリティ面で安全性が高く、各サイトへのログイン操作の負担を軽減することができる自動ログインシステムなどを提供することである。
【０００９】
【課題を解決するための手段】
本発明は、前記目的を達成するために、サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする自動ログイン装置を備えた自動ログインシステムであって、前記自動ログイン装置は、鍵情報を記憶したＩＣカードから前記鍵情報を取得する鍵情報取得手段と、自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて復号化する復号化手段と、前記復号化した自動ログイン情報を用いて前記サービスサイトに自動ログインする自動ログイン手段と、を具備したことを特徴とする自動ログインシステムを提供する（第１の構成）。
第１の構成で、前記自動ログイン情報の少なくとも一部を前記自動ログイン装置に提供する自動ログイン情報提供サーバを備えるように構成することができる（第２の構成）。
また、第１の構成において、前記ＩＣカードは、非接触型ＩＣカードであるように構成することができる（第３の構成）。
また、第１の構成において、前記自動ログイン装置は、前記自動ログイン情報記憶手段を具備するように構成することができる（第４の構成）。
また、第１の構成において、前記ＩＣカードは、前記自動ログイン情報の少なくとも一部を記憶しており、前記自動ログイン装置は、前記ＩＣカードから前記自動ログイン情報の

少なくとも一部を取得するように構成することができる（第５の構成）。
更に、第１の構成において、前記自動ログイン情報は、サービスサイト毎に構成されており、前記自動ログイン装置は、ユーザがサービスサイトを選択するサイト選択手段と、前記選択したサービスサイトに対する前記自動ログイン情報を検索する自動ログイン情報検索手段と、を具備し、前記自動ログイン手段は、前記検索した自動ログイン情報を用いて前記サービスサイトに自動ログインするように構成することができる（第６の構成）。
また、第１の構成において、前記自動ログイン情報は、自動ログイン対象のサービスサイトを特定するサービスサイト特定情報と、前記サービスサイト特定情報で特定される前記サービスサイトへのログイン処理を前記サービス提供サーバに要求するログインリクエスト情報と、を有する自動ログインサイト情報と、前記サービス提供サーバがユーザを認証するのに要するユーザ認証情報を有する自動ログイン個人情報と、から構成されているように構成することができる（第７の構成）。
また、第７の構成において、前記自動ログイン装置は、第２の鍵情報を取得する第２の鍵情報取得手段を具備し、前記自動ログイン個人情報は、前記ＩＣカードから取得した鍵情報と、前記取得した第２の鍵情報を用いて復号化可能に暗号化されており、前記復号化手段は、前記鍵情報と前記第２の鍵情報を用いて前記自動ログイン個人情報復号化するように構成することができる（第８の構成）。
また、第７の構成において、前記自動ログインサイト情報と、前記自動ログイン個人情報は、サービスサイト毎に対応付けられて構成されており、前記自動ログイン装置は、ユーザがサービスサイトを選択するサイト選択手段と、前記選択したサービスサイトに対する前記自動ログインサイト情報を検索する自動ログインサイト情報検索手段と、前記検索した自動ログインサイト情報に対応付けられた自動ログイン個人情報を検索する自動ログイン個人情報検索手段と、前記検索した自動ログインサイト情報に含まれるログインリクエスト情報と前記検索した自動ログイン個人情報に含まれるユーザ認証情報とを用いてサービス提供サーバがログイン処理を行うのに用いるログインリクエストを生成するログインリクエスト生成手段と、を具備し、前記自動ログイン手段は、前記生成したログインリクエストを前記選択したサービスサイトが設けられたサービス提供サーバに送信するように構成することができる（第９の構成）。
第８の構成において、前記自動ログイン装置は、前記検索された前記自動ログインサイト情報に対応する前記自動ログイン個人情報が検索できなかった場合、ユーザから入力される情報を用いて前記自動ログインサイト情報に対応する自動ログイン個人情報を、前記第１の鍵情報と前記第２の鍵情報で復号化可能に暗号化して追加する自動ログイン個人情報追加手段を具備するように構成することができる（第１０の構成）。
第７の構成において、前記自動ログイン装置が、前記自動ログイン情報を記憶する自動ログイン情報記憶手段を具備するように構成することができる（第１１の構成）。
第１１の構成において、前記自動ログイン情報記憶手段は、前記自動ログイン装置に着脱可能な記憶媒体に前記自動ログイン個人情報を記憶するように構成することができる（第１２の構成）。
第１０の構成において、請求項１０に記載の自動ログインサイト情報を前記自動ログイン装置に送信する自動ログインサイト情報提供サーバを備えるように構成することができる（第１３の構成）。
第１の構成において、前記自動ログイン装置は、前記ＩＣカードが前記自動ログイン装置にセットされているか否かを検出する検出手段と、前記検出手段で前記ＩＣカードがセットされていないと検出した場合に、前記自動ログイン装置に対する入力をロックするロック機構と、を具備するように構成することができる（第１４の構成）。
また、本発明は、前記目的を達成するために、第１２の構成に記載の記憶媒体であって、自動ログイン個人情報を記憶し、前記クライアント端末に着脱可能な記憶媒体を提供する。
また、本発明は、前記目的を達成するために、サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動

的にログインする自動ログイン装置を用いた自動ログイン方法であって、前記自動ログイン装置は、鍵情報取得手段と、復号化手段と、自動ログイン手段と、を備え、前記鍵情報取得手段で、鍵情報を記憶したＩＣカードから前記鍵情報を取得する鍵情報取得ステップと、自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて前記復号化手段で復号化する復号化ステップと、前記復号化した自動ログイン情報を用いて、前記自動ログイン手段で、前記サービスサイトに自動ログインする自動ログインステップと、から構成されたことを特徴とする自動ログイン方法を提供する（第１の方法）。

第１の方法において、自動ログイン情報提供サーバが、前記自動ログイン情報の少なくとも一部を前記自動ログイン装置に提供する自動ログイン情報提供ステップを備えるように構成することができる（第２の方法）。

第１の方法において、前記ＩＣカードは、非接触型ＩＣカードであるように構成することができる（第３の方法）。

第１の方法において、前記自動ログイン装置は、前記自動ログイン情報記憶手段を具備し、前記自動ログイン情報記憶手段から、前記自動ログイン情報を取得する自動ログイン情報取得ステップを備えるように構成することができる（第４の方法）。

第１の方法において、前記ＩＣカードは、前記自動ログイン情報の少なくとも一部を記憶しており、前記ＩＣカードから前記自動ログイン情報の少なくとも一部を取得する取得ステップを備えるように構成することができる（第５の方法）。

第１の方法において、前記自動ログイン情報は、サービスサイト毎に構成されており、前記自動ログイン装置は、サイト選択手段と、自動ログイン情報検索手段と、を備え、前記サイト選択手段で、ユーザがサービスサイトを選択するサイト選択ステップと、前記選択したサービスサイトに対する前記自動ログイン情報を、前記自動ログイン情報検索手段で検索する自動ログイン情報検索ステップと、を備え、前記自動ログインステップでは、前記検索した自動ログイン情報を用いて前記サービスサイトに自動ログインするように構成することができる（第６の方法）。

第１の方法において、前記自動ログイン情報は、自動ログイン対象のサービスサイトを特定するサービスサイト特定情報と、前記サービスサイト特定情報で特定される前記サービスサイトへのログイン処理を前記サービス提供サーバに要求するログインリクエスト情報と、を有する自動ログインサイト情報と、前記サービス提供サーバがユーザを認証するのに要するユーザ認証情報を有する自動ログイン個人情報と、から構成されているように構成することができる（第７の構成）。

第７の構成において、前記自動ログイン装置は、第２の鍵情報取得手段を具備し、前記第２の鍵情報取得手段で、第２の鍵情報を取得する第２の鍵情報取得ステップを備え、前記復号化ステップで、前記自動ログイン個人情報を、前記ＩＣカードから取得した鍵情報と、前記取得した第２の鍵情報を用いて復号化するように構成することができる（第８の構成）。

第７の構成において、前記自動ログインサイト情報と、前記自動ログイン個人情報は、サービスサイト毎に対応付けられて構成されており、前記自動ログイン装置は、サイト選択手段と、自動ログインサイト情報検索手段と、自動ログイン個人情報検索手段と、ログインリクエスト生成手段と、を具備し、前記サイト選択手段で、ユーザがサービスサイトを選択するサイト選択ステップと、前記自動ログインサイト情報検索手段で、前記選択したサービスサイトに対する前記自動ログインサイト情報を検索する自動ログインサイト情報検索ステップと、前記検索した自動ログインサイト情報に対応付けられた自動ログイン個人情報を、前記自動ログイン個人情報検索手段で検索する自動ログイン個人情報検索ステップと、前記検索した自動ログインサイト情報に含まれるログインリクエスト情報と前記検索した自動ログイン個人情報に含まれるユーザ認証情報とを用いてサービス提供サーバがログイン処理を行うのに用いるログインリクエストを前記ログインリクエスト生成手段で生成するログインリクエスト生成ステップと、前記生成したログインリクエストを前記選択したサービスサイトが設けられたサービス提供サーバに送信する送信ステップと、

を備えたるように構成することができる（第９の方法）。
第８の方法において、前記自動ログイン装置は、自動ログイン個人情報追加手段を具備し、前記検索された前記自動ログインサイト情報に対応する前記自動ログイン個人情報が検索できなかった場合、ユーザから入力される情報を用いて前記自動ログインサイト情報に対応する自動ログイン個人情報を、前記自動ログイン個人情報追加手段で、前記第１の鍵情報と前記第２の鍵情報で復号化可能に暗号化して追加する自動ログイン個人情報追加ステップを具備するように構成することができる（第１０の方法）。
第７の方法において、前記自動ログイン装置が、前記自動ログイン情報を記憶する自動ログイン情報記憶手段を具備し、前記自動ログイン情報記憶手段から、前記自動ログイン情報を取得する自動ログイン情報取得ステップを備えるように構成することができる（第１１の方法）。
第１１の方法において、前記自動ログイン情報取得ステップでは、前記自動ログイン装置に着脱可能な記憶媒体から前記自動ログイン個人情報を取得するように構成することができる（第１２の方法）。
第１０の方法において、自動ログインサイト情報提供サーバから、請求項２５に記載の自動ログインサイト情報を前記自動ログイン装置に送信する自動ログインサイト情報送信ステップを備えるように構成することができる（第１３の方法）。
第１の方法において、前記自動ログイン装置は、検出手段と、ロック機構とを具備し、前記検出手段で、前記ＩＣカードが前記自動ログイン装置にセットされているか否かを検出する検出ステップと、前記検出手段で前記ＩＣカードがセットされていないと検出した場合に、前記ロック機構で、前記自動ログイン装置に対する入力をロックするロックステップと、を備えるように構成することができる（第１４の方法）。
また、本発明は、前記目的を達成するために、サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする機能をコンピュータに発揮させるための自動ログインプログラムであって、鍵情報を記憶したＩＣカードから前記鍵情報を取得する鍵情報取得機能と、自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて復号化する復号化機能と、前記復号化した自動ログイン情報を用いて前記サービスサイトに自動ログインする自動ログイン機能と、をコンピュータで実現するための自動ログインプログラムを提供する。
更に、本発明は前記目的を達成するために、サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする機能をコンピュータに発揮させるための自動ログインプログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、鍵情報を記憶したＩＣカードから前記鍵情報を取得する鍵情報取得機能と、自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて復号化する復号化機能と、前記復号化した自動ログイン情報を用いて前記サービスサイトに自動ログインする自動ログイン機能と、をコンピュータで実現するための自動ログインプログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する。
【００１０】
【発明の実施の形態】
（第１の実施の形態）
以下、本発明の好適な第１の実施の形態について詳細に説明する。
（１）実施形態の概要
本実施の形態は、インターネットを介して提供される各サービスサイトへのログイン認証をＩＣカードのような記録媒体に記憶した鍵情報を用いるなどして自動的に行うものである。この鍵情報はログインする際に必要なログイン情報を復号化するのに用いられる。
ログイン情報を用いてログインすることにより、従来キーボードから入力していたログインＩＤとパスワードを入力する手間を省き、ユーザの負荷を軽減することができる。また、各サービスサイトへのログインには、ＩＣカードが必要となり、セキュリティ面でも安

全性を確保している。
本実施の形態の手法は、インターネット上のあらゆるサービスサイトへのログインで利用することができる。
【００１１】
クライアント端末３（図１）は、インターネット６を介してサービスＡ、Ｂ、　を提供するサーバ５、サーバ５、　（以下サーバ５）に接続可能に配設されている。サーバ５は、ユーザがログインを行うことにより、各種サービスを提供する。
クライアント端末３に搭載されたブラウザ１０は、自動ログイン部１２を備えており、自動ログイン情報１５を用いてサーバ５に自動的にログインする機能を備えている。
自動ログイン情報１５は、自動ログインサイト情報１６と、自動ログイン個人情報１７から構成されている。自動ログインサイト情報１６、自動ログイン個人情報１７は、何れも暗号化されており、自動ログインサイト情報１６は、ユーザが有する非接触ＩＣカード７に記憶されている第１の鍵情報９で復号化され、自動ログイン個人情報１７は、第１の鍵情報９と、ユーザが入力する自動ログイン用パスワード（第２の鍵情報）で復号化される。
【００１２】
自動ログインサイト情報１６（図２）は、サーバ５が提供するサービスを識別するサービス名称１４１、ログインページ（ログインＩＤやパスワードなどの認証情報をユーザが入力するためのログイン認証ページ）のＵＲＬであるログインページ情報１４２、ログインする際にサーバ５に送信する情報であるログインリクエスト情報１４３から構成されている。
一方、自動ログイン個人情報１７は、サーバ５が提供するサービスを識別するサービス名称１４５、ログインリクエスト情報１４３に付属させるパラメータ値（引数）１４６、１４７、１４８、　から構成されいる。各パラメータ値は、ユーザがサーバ５にログインする際に必要となるログインＩＤやパスワードなどのサーバ５がユーザを認証するための情報である。
自動ログインサイト情報１６と、自動ログイン個人情報１７は、サービス名称１４１とサービス名称１４５によりひも付けされており、一対一の対応関係がとられている。
【００１３】
自動ログイン部１２は、ブラウザ１０に入力されたＵＲＬを監視しており、入力されたＵＲＬがログインページに登録されているＵＲＬに一致すると、その該当するサービス名称１４１のログインリクエスト情報１４３のパラメータに、自動ログイン個人情報１７のパラメータ値１４６、１４７、　を代入してログインリクエストを生成し、サーバ５に送信する。
サーバ５は、クライアント端末３からログインリクエストを受け取り、これを用いてユーザを認証し、ログイン処理（ログイン認証処理）を行う。
【００１４】
このように、ブラウザ１０に入力されるＵＲＬを監視して、その結果、接続先のサービスサイトが自動ログイン情報１５に登録してあるものである場合、自動的にログインを行うことができる。そのため、ブラウザ１０は、ログイン手続きでユーザが行う負担を軽減することができる。
更に、今後、インターネットブラウザ機能を持ったテレビなどの情報家電の普及が予想される。このような情報家電は通常キーボードなどの入力デバイスを持たない場合が多いと考えられ、その場合、リモコンを用いてログインＩＤとパスワードを入力すると思われる。この場合、ログインＩＤとパスワードの入力がユーザにとって負担になると共に、ログインＩＤやパスワードが第三者の手に渡った場合、どのクライアント端末からでもログインＩＤとパスワードを入力することが可能であり、セキュリティ的にも問題がある。
これら情報家電に、本実施の形態のブラウザ１０を搭載すると、ユーザは、非接触ＩＣカード７と自動ログイン用パスワードを用いて自動的にログインすることになり、これらのパラメータの入力が容易になると共に、セキュリティを高めることができる。

【００１５】
（２）実施形態の詳細
図１は、本実施の形態のシステム構成を説明するための図である。
自動ログインシステム１は、非接触ＩＣカード７、クライアント端末３、インターネット６、自動ログインサイト情報提供サーバ４、サーバ５、５、　（以下サーバ５）から構成されている。
非接触ＩＣカード７は、非接触でデータの送受信を行うデータ送受信手段、受信したデータを記憶する記憶手段などを備えており、クライアント端末３に設けられたＩＣカードＲＷ（リーダライタ）２１を介して、クライアント端末３とデータの送受信を行うことができる。また、演算手段を備えることも可能である。
非接触ＩＣカード７は、ループ状のアンテナと半導体チップを内蔵しており、ＩＣカードＲＷ２１に近づけると、ＩＣカードＲＷ２１が発する電磁波をこのアンテナで受信して起電力を得ると共に、データの送受信を行う。
【００１６】
本実施の形態では、非接触ＩＣカード７に第１の鍵情報９を記憶しておき、これをＩＣカードＲＷ２１で読み取る。
第１の鍵情報９は、暗号鍵などの鍵情報を非接触ＩＣカード７に記憶さてもよいし、あるいは、非接触ＩＣカード７に予めＩＣカードＲＷ２１で読み取り可能に割り当てられている固有ＩＤを用いてもよい。固有ＩＤは、非接触ＩＣカード７毎に一意的に割り当ててあり、固有ＩＤにより、非接触ＩＣカード７を特定することができる。本実施の形態では、固有ＩＤを第１の鍵情報９として用いるものとする。このように、ＩＣカードＲＷ２１は鍵情報取得手段を構成している。
【００１７】
クライアント端末３は、ブラウザ１０、自動ログイン情報１５、ＩＣカードＲＷ２１、パスワード入力部２２、ブラウザ操作部２３を備えており、インターネット６を介して、自動ログインサイト情報提供サーバ４（自動ログイン情報提供サーバ）、サーバ５に接続可能に配設されている。
詳細は後述するが、クライアント端末３は、例えば、パーソナルコンピュータを用いて構成されている。
ブラウザ１０は起動するとＩＣカードＲＷ２１を監視し、非接触ＩＣカード７がＩＣカードＲＷ２１に接近すると、非接触ＩＣカード７から第１の鍵情報９を読み取り、ブラウザ１０に渡す。ブラウザ１０は、一定時間毎に非接触ＩＣカード７の有無を監視している。
パスワード入力部２２は、例えば、ディスプレイに表示された自動ログインパスワード入力ダイアログと、キーボードなどから構成され、ユーザがキーボードなどから入力した自動ログインパスワードを取得する。パスワード入力部２２で取得した自動ログインパスワードは、後述する第２の鍵情報として使用される。
このように、パスワード入力部２２は、第２の鍵情報取得手段を構成している。
【００１８】
ブラウザ操作部２３は、ブラウザ１０が備えた各機能を操作するためのユーザインターフェースであり、例えば、ディスプレイに表示されたブラウザ画面、情報を入力するためのキーボード、マウスなどから構成される。
ユーザは、ブラウザ画面を見ながら、キーボード、マウスなどから情報を入力し、ブラウザ１０が備えた各機能を操作することができる。
ブラウザ操作部２３からのＵＲＬの入力は、例えば、サービスサイトを表したアイコンをクリックしたり、あるいはブラウザ画面上に設けられたＵＲＬ欄にキーボードからＵＲＬを入力するなどして行うことができる。
また、ユーザがホームページでログインページにジャンプするボタンをクリックした場合、サーバ５からログインページが送信されてきて、ＵＲＬ欄にこのログインページのＵＲＬが入力される。
【００１９】

ブラウザ１０は、ブラウザ機能部１１と自動ログイン部１２から構成されている。ブラウザ機能部１１は、通常のブラウズを行う機能部であり、インターネット６上に開設されたサービスサイトにアクセスして、これらサービスサイトが提供するサービスを利用するのに用いる。
ブラウザ機能部１１は、例えば、入力されたＵＲＬで指定されるサービスサイトにアクセスし、これに対してサービスサイトが送信してくるホームページを表示する。
また、ユーザがこれらホームページ上で入力した情報を所定のサーバ５に送信する。
ユーザは、ブラウザ機能部１１を用いてサービスサイトが提供するサービスを利用することにより、例えば、必要な情報を検索したり、オンラインショッピングを行ったり、あるいは、預金口座や株式売買を管理したり、更には、ゲームや動画を見たりなど、様々なコンテンツを利用することができる。
【００２０】
自動ログイン部１２は、ユーザがログイン認証を要するサービスサイトにアクセスした際に、ログイン認証手続きを自動的に行い代行する機能部である。
詳細は後述するが、自動ログイン部１２は、ブラウザ機能部１１がアクセスするＵＲＬを監視しており、後述の自動ログインサイト情報１６に登録してあるＵＲＬ（ログインページのＵＲＬ）にアクセスした場合に、ユーザに代わってログインリクエストを作成してサーバ５に送信する。
ログインリクエストとは、サーバ５側で、ログイン処理を行う認証処理プログラム（例えばＣＧＩ（Ｃｏｍｍｏｎ Ｇａｔｅｗａｙ Ｉｎｔｅｒｆａｃｅ）プログラムにより構成される）を動作させ、ユーザを認証させるための情報である。通常は、ユーザがログイン画面で入力したログインＩＤ、パスワードなどをパラメータ値としてサーバ５に送信する。サーバ５では、このログインリクエストによりログイン認証プログラムを動作させ、ログインリクエストに付属するパラメータ値（ログインＩＤ、パスワードなど）を用いてユーザをログイン認証する。
【００２１】
自動ログイン情報１５は、自動ログイン部１２がＵＲＬを監視したり、ログインリクエストを自動生成するのに用いる情報から構成されている。
後に詳細に説明するが、自動ログインサイト情報１６は、ログインページやログインリクエストを生成するためのログインリクエスト情報など、公になっている情報から構成されている。
自動ログインサイト情報１６は、非接触ＩＣカード７から取り込んだ第１の鍵情報９で復号化可能に暗号化されている。自動ログインサイト情報１６は、後述する自動ログインサイト情報提供サーバ４からインターネット６を経由してダウンロードしたものである。また、自動ログインサイト情報提供サーバ４から更新情報を受信し、これを用いてクライアント端末３は自動ログインサイト情報１６を最新のものに更新することができる。
自動ログイン個人情報１７は、ログインＩＤやパスワードなど、ユーザに固有なユーザ認証用の情報（ユーザ認証情報）などから構成されている。
自動ログイン個人情報１７は、第１の鍵情報９、及びパスワード入力部２２から取得した自動ログインパスワードの双方を用いて復号化できるように暗号化されている。この場合、自動ログインパスワードは、第２の鍵情報を構成している。
【００２２】
自動ログインサイト情報提供サーバ４は、クライアント端末３に自動ログインサイト情報１６や、自動ログインサイト情報１６を更新するための更新情報を提供するためのサーバ装置である。
自動ログインサイト情報提供サーバ４では、自動ログインサイト情報提供サーバ４の事業者が、クライアント端末３で自動ログインサイト情報１６に新たなサービスサイトを追加したり、あるいは削除したりするための更新情報を管理している。
この更新情報は、クライアント端末３で、自動ログインサイト情報１６を全て上書きするように構成することもできるし、あるいは、最新の自動ログインサイト情報と、クライア

ント端末３の自動ログインサイト情報１６の差分を送るように構成することもできる。
【００２３】
サーバ５、５、　は、サービスＡ、サービスＢ、　など、各種のサービスを提供するサービスサイトが開設されたＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）サーバである。図１では、それぞれのサーバ５に１つずつサービスサイトが開設されているが、サービスサイトはＵＲＬにより一意的に識別できるため、１つのサーバ５に複数のサービスサイトを開設してもよい。
本実施の形態のサービスＡ、サービスＢ、　を提供するサービスサイトは、ユーザからログインＩＤやパスワードなどの個人認証用の情報を受け取ってログイン認証を行うものとする。
【００２４】
サービスサイトで提供されるサービスは、例えば、銀行口座の管理、有価証券の売買、電子メールの送受信、オンラインショッピング、会員それぞれ用にカスタマイズされたテレビ番組表、会員制の娯楽サイト、　など各種のものが考えられる。本実施の形態では、何れのサービスサイトもログイン認証を必要とするものである。また、サービスサイトには、有料のものや無料のものがある。
なお、本実施の形態では、自動ログインに関する処理はクライアント端末３が行うため、サーバ５に自動ログイン用の仕組みを設けるなど、サーバ側の変更は必要ない。
【００２５】
本実施の形態では、ネットワークとしてインターネット６を考えたが、これに限定するものではなく、例えば、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、人工衛星を介したネットワークなど、他の形態のネットワークでもよい。
なお、サーバ５をＷＷＷサーバとしたが、これに限定するものではなく、ユーザから個人認証用の情報を受信してログイン認証する送受信装置であればよい。
また、本実施の形態では、非接触ＩＣカード７を用いたが、接触式のＩＣカード、ＩＤカードなど、クライアント端末３が第１の鍵情報９を読み出せる他の記憶媒体を用いてもよい。
更に、第２の鍵情報を得るために、パスワード入力部２２から自動ログインパスワードを取得したが、第２の鍵情報の取得方法は、これに限定するものではなく、例えば、ユーザの指紋、声紋、目の虹彩など、ユーザを確認できるものであればよい。
【００２６】
図２は、自動ログイン情報１５の論理的な構成の一例をテーブルとして示した図である。このうち、図２（ａ）は、自動ログインサイト情報１６を示し、図２（ｂ）は、自動ログイン個人情報１７を示している。
図２（ａ）に示したように、自動ログインサイト情報１６は、サービス名称１４１、ログインページ情報１４２、ログインリクエスト情報１４３から構成されており、サービス名称１４１毎に区分されている。
自動ログインサイト情報１６は、第１の鍵情報９により復号化可能に暗号化されている。
サービス名称１４１は、自動ログインサイト情報１６と自動ログイン個人情報１７とをひも付けして対応させるための情報であり、ここでは、サービスサイトに一意的に割り当てられたサービス名称を用いている。
【００２７】
ログインページ情報１４２は、自動ログイン処理の対象となるサービスサイトのログインページのＵＲＬである。ログインページ情報１４２は、自動ログイン部１２（図１）が、ブラウザ機能部１１で入力されたＵＲＬを監視するために用いる。
即ち、自動ログイン部１２は、ブラウザ機能部１１でＵＲＬが入力されると、このＵＲＬとログインページ情報１４２を比較し、一致するものがある場合に、自動ログイン処理を行う。
【００２８】

ログインページ情報１４２に登録されているＵＲＬは、例えば、「ｈｔｔＰ：／／ｓｅｒｖｅｒＡ．ｃｏｍ／ｌｏｇｉｎ．ｈｔｍｌ」といったように構成されており、この場合、サーバ「ｓｅｒｖｅｒＡ」にあるＨＴＭＬ（ＨｙＰｅｒｔｅｘｔ　ＭａｒｋｕＰ　Ｌａｎｇｕａｇｅ）ファイル「ｌｏｇｉｎ．ｈｔｍｌ」を特定している。
なお、ＨＴＭＬファイル「ｌｏｇｉｎ．ｈｔｍｌ」は、ブラウザ機能部１１にログインページ画面を表示させるための画面データである。

【００２９】

ログインリクエスト情報１４３は、サーバ５がログイン認証を行うのに用いるログインリクエストを生成するための情報である。
ログインリクエストは、サーバ５でログイン処理を要求するための情報であり、一般にパラメータ値（引数）としてログインＩＤやパスワードなどを伴う。
ログインリクエスト情報１４３は、例えば、「ｈｔｔＰＳ：／／ｓｅｒｖｅｒＡ．ｃｏｍ／ｌｏｇｉｎ．ｃｇｉ？Ｌｉｄ％＝１Ｐｗｄ＝％２」といったような形をしている。
これは、サーバ「ｓｅｖｅｒＡ」のログイン認証プログラム「ｌｏｇｉｎ．ｃｇｉ」に、パラメータ「％１」に付属するパラメータ値（ログインＩＤ）と、パラメータ「％２」に付属するパラメータ値（パスワード）を引数として渡すことを意味している。
本実施の形態では、「％１」や「％２」などのパラメータに付属させるログインＩＤやパスワードなどのパラメータ値は、次に説明する自動ログイン個人情報１７で管理している。

【００３０】

図２（ｂ）に示したように、自動ログイン個人情報１７には、サービス名称１４５や、パラメータ値１４６、１４７、その他のパラメータ値１４８　などの、ユーザを認証する際に使用するユーザに固有な情報などが含まれている。
自動ログイン個人情報１７は、サービス名称１４５毎に区分されており、第１の鍵情報９、及び第２の鍵情報（自動ログインパスワード）で復号化可能に暗号化されている。このように、自動ログイン個人情報１７には、ユーザに固有な情報が含まれているため、第１の鍵情報９と第２の鍵情報を用いないと復号化できないようになっており、セキュリティが高められている。
このため、第三者が非接触ＩＣカード７を取得して第１の鍵情報９を利用しても、自動ログインパスワードがわからなければ、自動ログイン個人情報１７を復号化することはできない。

【００３１】

サービス名称１４５は、自動ログインサイト情報１６とひも付けするための情報であり、サービスサイトに一意的に与えられたサービス名称である。
自動ログイン部１２は、サービス名称１４１と同じサービス名称１４５を検索することにより、自動ログインサイト情報１６と自動ログイン個人情報１７をひも付けすることができる。

【００３２】

パラメータ値１４６は、ひも付けされたログインリクエスト情報１４３のパラメータ「％１」に付属させるためのパラメータ値であり、通常はログインＩＤが用いられる。
パラメータ１４７は、ひも付けされたログインリクエスト情報１４３のパラメータ「％２」に付属させるためのパラメータ値であり、通常はパスワードが用いられる。
なお、「％１」にどのパラメータ値を対応させるかは、サーバ５で設定できるため、サーバ５によっては、「％１」にパスワードなど他のパラメータ値が設定されている場合もある。
その他のパラメータ値１４８は、ログインリクエスト情報１４３が更に多くのパラメータ値を必要とする場合に、そのパラメータ値が設定される。このような場合として、例えば、１回のログイン処理に複数のパスワードを使用する場合などがある。

【００３３】

図３は、ブラウザ１０の機能的な構成を説明するための模式図である。

図３に示したように、ブラウザ１０は、ブラウザ機能部１１、暗号・復号部３１、自動追加部３２、ログインリクエスト生成部３３、ログインリクエスト送信部３４、ブラウザ監視部３５などから構成されている。
これらの機能部は、後述するブラウザプログラム５６（図４）をＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）４１で実行することにより、ソフトウェア的に構成される。
【００３４】
より詳細には、ブラウザ１０は、ブラウザ機能部１１に自動ログイン部１２をプラグインソフトとして組み込んで構成することもできる。この場合、自動ログイン部１２を汎用的に使用されているインターネットブラウザの拡張アプリケーションとすることができる。あるいは、自動ログイン部１２とブラウザ機能部１１を有するブラウザ１０をプログラミングすることにより構成してもよい。
【００３５】
ブラウザ１０の、ブラウザ機能部１１はブラウザ１０が起動している間中動作する。一方、自動ログイン部１２は、ＩＣカードＲＷ２１に非接触ＩＣカード７がセットされている間だけ動作するように構成されている。
以上のように、動作するために、ブラウザ１０は、ＩＣカードＲＷ２１に非接触ＩＣカード７がセットされているか否かを監視している。
【００３６】
暗号・復号部３１は、自動ログイン情報１５の復号化、及び暗号化を行う機能部である。暗号・復号部３１は、復号化手段、暗号化手段を構成している。
暗号・復号部３１は、ＩＣカードＲＷ２１が非接触ＩＣカード７から読み取った第１の鍵情報９を取得し、自動ログインサイト情報１６を復号化する。復号後の自動ログインサイト情報１６は、ＲＡＭなどに記憶する。この復号化した自動ログインサイト情報１６により、ブラウザ１０は、自動ログインサイト情報１６を利用できるようになる。
また、暗号・復号部３１は、第１の鍵情報９を用いて自動ログインサイト情報１６を第１の鍵情報９で復号化可能に暗号化することもできる。これにより、自動ログインサイト情報提供サーバ４からダウンロードした最新の自動ログインサイト情報（暗号化されていない）を暗号化して自動ログイン情報１５に格納することができる。
【００３７】
なお、クライアント端末３から自動ログインサイト情報提供サーバ４にユーザを特定する情報を提供し（これにより自動ログインサイト情報提供サーバ４は、このユーザが使用している第１の鍵情報９がわかるものとする）、第１の鍵情報９で復号化可能に暗号化した自動ログインサイト情報１５を自動ログインサイト情報提供サーバ４からクライアント端末３に送信するように構成してもよい。この場合は、暗号・復号部３１に自動ログインサイト情報１６を暗号化する機能を搭載する必要は必ずしもなくなる。
更に、暗号・復号部３１は、第１の鍵情報９と、パスワード入力部２２から取得した第２の鍵情報（自動ログインパスワード）を用いて自動ログイン個人情報１７を復号化すると共に、復号化された自動ログイン個人情報１７をこれらの鍵情報で復号化可能に暗号化することができる。復号化した自動ログイン個人情報１７は、例えば、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）などに記憶する。
【００３８】
このように、暗号・復号部３１は、自動ログインサイト情報１６、自動ログイン個人情報１７を復号化して、他の構成要素からアクセス可能に、ＲＡＭなどのメモリに記憶することができる。
なお、本実施の形態では、自動ログイン個人情報１７が第１の鍵情報９と第２の鍵情報の双方を用いて復号化可能としたが、これに限定するものではなく、第２の鍵情報により復号化できるように構成してもよい。
【００３９】
ブラウザ機能部１１は、一般のＷＷＷブラウザと同様に、ＷＷＷサーバが提供するサービ

スをユーザに利用可能に提供する機能部である。
より詳細には、ブラウザ画面（例えば、ＵＲＬ欄を備え、ＨＴＭＬファイルが定義した解釈した画面を表示する画面）をディスプレイに表示することができ、また、ブラウザ画面上のＵＲＬ欄に入力してあるＵＲＬで特定されるファイルをこのファイルが保存されているＷＷＷサーバからダウンロードする。
所定のファイルには、例えばＨＴＭＬファイルやＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）ファイルなどのマークアップ言語で構成されたものがあり、この場合、ブラウザ機能部１１は、これらファイルで定義されている画面をディスプレイに表示する。
ブラウザ機能部１１は、サイト選択手段を構成している。

【００４０】
ＵＲＬ欄には、現在ブラウザ画面に表示されているＷｅｂページのＵＲＬが表示されており、ＵＲＬに新たなＵＲＬを入力して変更すると、新規入力したＵＲＬで特定されるファイルがダウンロードされる。
ＵＲＬ欄へのＵＲＬの入力は、ユーザがキーボードから入力することもできる。また、この他に、特定のＵＲＬが設定されたアイコンなどのシンボルをブラウザ画面上に配置し、これをユーザがマウス操作でクリックするなどして選択することにより、このアイコンなどに設定されているＵＲＬをＵＲＬ欄に入力することもできる。

【００４１】
ブラウザ監視部３５は、ブラウザ機能部１１のＵＲＬ欄を監視し、ＵＲＬ欄に入力されているＵＲＬが、自動ログインサイト情報１６のログインページ情報１４２（図２）に登録されているＵＲＬと一致するか否かを監視している。そして、一致するＵＲＬがあった場合、一致したログインページ情報１４２を特定する特定情報をログインリクエスト生成部３３に送る。

【００４２】
ログインリクエスト生成部３３は、ブラウザ監視部３５からこの特定情報を受け取り、これを用いてログインリクエストの生成を行う。
ログインリクエスト生成部３３は、受け取った特定情報と、ログインページ情報１４２とをマッチングし、サービス名称１４１とログインリクエスト情報１４３を特定する。

【００４３】
更に、ログインリクエスト生成部３３は、特定されたサービス名称１４１とサービス名称１４５をマッチングし、ログインリクエスト情報１４３のパラメータとして設定するパラメータ値（パラメータ値１４６、１４７、１４８、　）を取得する。
そして、ログインリクエスト生成部３３は、ログインリクエスト情報１４３と取得したパラメータ値からログインリクエストを生成し、ログインリクエスト送信部３４に送る。
ログインリクエストの生成は、ログインリクエスト情報１４３のパラメータ（％１、％２、　）に自動ログイン個人情報１７で特定されたパラメータ値を代入する（付属させる）ことにより行う。

【００４４】
また、ログインリクエスト生成部３３は、自動ログインサイト情報１６のサービス名称１４１に対応する（ひも付けされた）サービス名称１４５が自動ログイン個人情報１７で見つからなかった場合、そのサービス名称１４１とログインリクエスト情報１４３を自動追加部３２に送る。
これは、自動ログインサイト情報１６は自動ログインサイト情報提供サーバ４で既に作成されたものであるので、最初にこれに対するパラメータ値をユーザが入力して自動ログイン個人情報１７を作成する必要があるためである。
ログインリクエスト生成部３３は、自動ログイン情報検索手段、自動ログインサイト情報検索手段、自動ログイン個人情報検索手段、ログインリクエスト生成手段を構成している。

【００４５】

自動追加部３２は、ログインリクエスト情報１４３に登録されているが、まだ自動ログイン個人情報１７に登録されていないサービスサイトに関して、ユーザに自動ログイン個人情報１７へのパラメータ値の入力を促すと共に、ユーザがログインページで入力したパラメータ値を用いて当該サービスサイトに関する情報を自動ログイン個人情報１７に追加する。
自動追加部３２は、この追加を、ＲＡＭなどに記憶した復号化済みの自動ログイン個人情報１７に対して行う。そして、後ほど、暗号・復号部３１は、これを暗号化し、暗号化された自動ログイン個人情報１７を更新する。
【００４６】
より詳細に説明すると、ユーザが自動ログインサイト情報１６に登録されていて自動ログイン個人情報１７に登録されていないサービスサイトのログインページにアクセスすると、自動追加部３２は、「自動ログインに設定しますか？」などといった適当な表示をブラウザ画面に表示し、このログインページが自動ログイン対象であることを知らせる。ここで、ユーザは登録するか否かを選択することができるようになっている。
そして、ユーザが登録を選択した場合、自動追加部３２は、ユーザがログインＩＤやパスワードを入力するためのダイアログを表示し、ユーザからパラメータ値を取得する。
【００４７】
あるいは、ログインページ（一般にログインＩＤ入力欄やパスワード入力欄などを備えている）でユーザが入力するパラメータ値を観察し、これとログインリクエスト情報１４３とを比較して、どのパラメータにどのパラメータ値（ログインＩＤ、パスワード）が入力されるかを把握する。そして、自動追加部３２は、把握したパラメータ値と、ログインリクエスト生成部３３から受け取ったサービス名称１４１を用いて自動ログイン個人情報１７を更新することも可能である。自動追加部３２と暗号・復号部３１は、自動ログイン個人情報追加手段を構成している。
【００４８】
ログインリクエスト送信部３４は、ログインリクエスト生成部３３から受け取ったログインリクエストをログインページを送ってきたサーバ５に送信する。
本実施の形態では、ログインリクエスト送信部３４がサーバ５にログインリクエストを送信するように構成したが、これに限定するものではなく、例えば、ログインリクエスト送信部３４からブラウザ機能部１１にログインリクエストを渡し、ブラウザ機能部１１からサーバ５にログインリクエストを送信するように構成してもよい。
ログインリクエスト生成部３３、ログインリクエスト送信部３４は、自動ログイン手段を構成している。
【００４９】
図４は、クライアント端末３のハードウェア的な構成の一例を説明するための図である。
クライアント端末３は、例えばパーソナルコンピュータを用いて構成されており、ＣＰＵ４１にバスライン４９を介して、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）４２、ＲＡＭ４３、表示手段４５、入力手段４６、出力手段４７、通信制御手段４８、記憶装置５５、記憶媒体駆動装置５２、入出力Ｉ／Ｆ（インターフェース）５１、ＩＣカードＲＷ２１などの周辺機器が接続して構成されている。
バスライン４９は、ＣＰＵ４１と周辺機器の間で送受信される制御信号やデータ信号の送受信を媒介する。
【００５０】
ＣＰＵ４１は、後述のブラウザプログラム５６に従って動作し、サーバ５へアクセスしたり、また、自動ログイン処理を行ったりする。また、ＯＳ（ＯＰｅｒａｔｉｎｇ ＳＹＳｔｅｍ）などに従って、クライアント端末３全体を制御したりなど、各種情報処理や制御を行う。
ＲＯＭ４２は、ＣＰＵ４１が各種演算や制御を行うための各種プログラム、データ及びパラメータなどを格納した読み取り専用の記憶装置である。ＣＰＵ４１は、ＲＯＭ４２からプログラムやデータ、パラメータなどを読み込むことはできるが、これらを書き換えたり

消去したりすることを行わない。
【００５１】
ＲＡＭ４３は、ＣＰＵ４１にワーキングメモリとして使用される読み書き可能な記憶装置である。ＣＰＵ４１は、ＲＡＭ４３にプログラムやデータなどを書き込んだり消去したりすることができる。本実施の形態では、ＲＡＭ４３には、復号化された自動ログインサイト情報１６や、自動ログイン個人情報１７を記憶したり、ログインリクエストを生成したりなどするためのエリアが確保可能となっている。
【００５２】
表示手段４５は、ブラウザ画面などの表示情報を表示するための手段であり、例えばＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ）ディスプレイ、液晶ディスプレイ、プラズマディスプレイなどのディスプレイで構成されている。
入力手段４６は、例えばキーボードやマウスなどの入力装置から構成されている。
キーボードは、クライアント端末３に対して文字や数字などの情報を入力するための装置である。キーボードは、カナや英文字などを入力するためのキーや数字を入力するためのテンキー、各種機能キー、カーソルキー及びその他のキーによって構成されている。ユーザは、キーボードからＵＲＬや、ログインＩＤ、パスワードなどを入力することができる。
マウスは、ポインティングデバイスである。ＧＵＩ（ＧｒａＰｈｉｃａｌ　Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）などを用いてクライアント端末３を操作する場合、表示装置上に表示されたボタンやアイコンなどをマウスでクリックすることにより、所定の情報（ＵＲＬなど）の入力を行うことができる。
出力手段４７は、例えば印刷装置などの出力装置から構成されている。
【００５３】
通信制御手段４８は、インターネット６を介してクライアント端末３を自動ログインサイト情報提供サーバ４やサーバ５などに接続するための装置であって、モデム、ターミナルアダプタ、その他の装置によって構成されている。
通信制御手段４８はＣＰＵ４１によって制御され、所定のプロトコルに従ってサーバ５や自動ログインサイト情報提供サーバ４などと信号やデータの送受信を行い、ログインリクエストの送信やサービスサイトが提供する情報を受信したりすることができる。
【００５４】
記憶媒体駆動装置５２は、着脱可能な記憶媒体を駆動してデータの読み書きを行うための駆動装置である。着脱可能な記憶媒体としては、例えば、光磁気ディスク、磁気ディスク、磁気テープ、半導体メモリ、データをパンチした紙テープ、ＣＤ－ＲＯＭなどがある。
なお、ＣＤ－ＲＯＭや紙テープは、読み込みのみ可能である。
なお、自動ログインサイト情報１６は、自動ログインサイト情報提供サーバ４からダウンロードするのではなく、記憶媒体の形で事業者に配布してもらい、記憶媒体駆動装置５２を介してクライアント端末３に取り込むこともできる。
【００５５】
記憶装置５５は、読み書き可能な記憶媒体と、その記憶媒体に対してプログラムやデータを読み書きするための駆動装置によって構成されている。当該記憶媒体として主にハードディスクが使用されるが、その他に、例えば、光磁気ディスク、磁気ディスク、半導体メモリなどの他の読み書き可能な記憶媒体によって構成することも可能である。
【００５６】
記憶装置５５は、ブラウザプログラム５６、自動ログインサイト情報データベース５７、自動ログイン個人情報データベース５８などを記憶している。
ＣＰＵ４１は、記憶装置５５の駆動装置を駆動することにより、記憶装置５５に対してプログラムやデータの読み込みや書き出しを行うことができる。
記憶装置は、自動ログイン情報記憶手段を構成している。
【００５７】
ブラウザプログラム５６は、ＣＰＵ４１にブラウザ機能を発揮させるためのプログラムで

ある。ブラウザプログラム５６がＣＰＵ４１に読み込まれて実行されることにより、図３に示した暗号・復号部３１からブラウザ監視部３５、及びブラウザ機能部１１の各構成要素がソフトウェア的に構成される。
自動ログインサイト情報データベース５７と、自動ログイン個人情報データベース５８は、それぞれ暗号化された自動ログインサイト情報１６、自動ログイン個人情報１７を格納するデータベースである。
【００５８】
自動ログインサイト情報データベース５７に格納する自動ログインサイト情報１６は、通信制御手段４８を介して自動ログインサイト情報提供サーバ４からダウンロードしたものである。
図示しないが、記憶装置５５には、例えば、通信制御手段４８を制御し、クライアント端末３とネットワークでつながれた端末装置やサーバ装置との通信を維持する通信プログラムや、メモリ管理や入出力管理などのクライアント端末３を動作させるための基本ソフトウェアであるＯＳ、及びＩＣカードＲＷ２１のドライバソフトなどの各種プログラムや、その他のデータが記憶されている。
【００５９】
入出力Ｉ／Ｆ５１は、例えば、シリアルインターフェースやその他の規格のインターフェースにより構成されている。入出力Ｉ／Ｆ５１に当該インターフェースに対応した外部機器を接続することにより、クライアント端末３の機能を拡張することができる。このような外部機器として例えば、ハードディスクなどの記憶装置、スピーカ、マイクロフォンなどがある。
ＩＣカードＲＷ２１は、非接触ＩＣカード７とデータの送受信を行ったり、非接触ＩＣカード７に電力を供給するアンテナが備えられている。
【００６０】
本実施の形態では、クライアント端末３は、例えば、パーソナルコンピュータで構成されているが、これに限定するものではなく、インターネット接続機能を持った情報家電（テレビ、ＣＥ機器）など、各種のハードウェアで構成することができる。
例えば、インターネット接続機能を持ったテレビの場合、テレビ画面が表示手段４５を構成し、赤外線式のリモートコントローラが入力手段４６を構成する。
ユーザは、テレビ画面に表示されたブラウザ画面を見ながら、リモートコントローラで情報を入力する。
【００６１】
図５は、ブラウザ１０が自動ログインを行う手順を説明するためのフローチャートである。
なお、以下のフローチャートで各構成要素が行う動作は、ＣＰＵ４１がブラウザプログラム５６に従って動作することにより実現されるものである。
ここで、非接触ＩＣカード７は、ＩＣカードＲＷ２１にまだセットされておらず、自動ログインサイト情報１６、自動ログイン個人情報１７の何れもまだ復号化されていないものとする。
【００６２】
ブラウザ１０は、ＩＣカードＲＷ２１に非接触ＩＣカード７がセットされているか否かを監視しており、非接触ＩＣカード７がセットされると、自動ログイン部１２を起動する（ステップ１１００）。そして、暗号・復号部３１は、第１の鍵情報９を非接触ＩＣカード７から取得して自動ログインサイト情報１６を復号化し、ＲＡＭ４３に記憶する。更に、ブラウザ監視部３５が、ブラウザ機能部１１を監視し始め、ブラウザ画面のＵＲＬ欄に入力される値をチェック（確認）する（ステップ１２００）。
なお、ブラウザ１０は、非接触ＩＣカード７がＩＣカードＲＷ２１にセットしてある間も、一定時間毎に非接触ＩＣカード７がセットされているか否かを監視しており、非接触ＩＣカード７がＩＣカードＲＷ２１から取り外されると、自動ログイン部１２の機能を終了させる。

【００６３】
次に、ユーザは、ホームページ上のクリックボタン（ログインページにジャンプするように設定されているもの）をクリックするなどしてログインページにアクセスする（ステップ１１０５）。これに対して、サーバ５は、ログインページをクライアント端末３に送信する（ステップ１３００）。
図６（ａ）は、ユーザがログインページを要求する際に、ブラウザ画面に表示されるホームページの一例を示したものである。
ユーザは、サービスＡを提供するサービスサイトにアクセスし、ページ１０１を表示させ、ログインボタン１０２をクリックすると、サーバ５からログインページが送信されくる。ブラウザ１０がログインページを受け取ると、ＵＲＬ欄にログインページのＵＲＬが入力される。
ここで、このログインページは自動ログインサイト情報１６で登録されているものであるとする。
【００６４】
図５に戻り、自動ログイン部１２は、ＵＲＬ欄に入力された値をチェックし（ステップ１２０５）、これがログインページ情報１４２に登録されたＵＲＬにマッチングするので、ブラウザ画面上にこのサービスサイトが自動ログイン対象である旨の自動ログイン可能通知を行う（ステップ１１１０）。
図６（ｂ）は、自動ログイン可能通知の一例を示した図である。
ログインページ１０５は、サーバ５がログイン処理するためのログインＩＤを入力するログインＩＤ入力欄１０６と、パスワードを入力するためのパスワード入力欄１０７を備えている。これらは、サーバ５がクライアント端末３に送信した画面データにより構成されたものである。そして、これらの欄の上に、「ＩＣカードで自動ログインできます。」といった自動ログイン可能通知が表示されている。この部分は、自動ログイン部１２がブラウザ機能部１１に表示させたものである。
ユーザは、ログイン通知により、これからログインしようとしているサービスサイトが自動ログイン対象であることを知ることができる。
【００６５】
図５に戻り、ブラウザ機能部１１は、自動ログイン可能通知した後、自動ログインパスワード入力画面を表示し、自動ログインパスワードの入力をユーザに促す。そして、ユーザがパスワード入力部２２から自動ログインパスワードを入力すると（ステップ１１１５）、自動ログイン部１２がこれを取得し、これが正しいものであるか否かを照合する（ステップ１２１０）。なお、照合用の自動ログインパスワードは、予め記憶装置５５やＲＯＭ４２などに格納しておく。
ここでは、自動ログインパスワードは正常に照合されたものとする。
【００６６】
図６（ｃ）は、自動ログインパスワード入力画面の一例を示した図である。図に示したように、自動ログインパスワード入力画面１１０では、「自動ログイン用のパスワードを入力してください。」などと、自動ログインパスワードの入力をユーザに促す表示が行われると共に、自動ログインパスワード入力欄１１１が表示される。ユーザが自動ログインパスワード入力欄１１１に自動ログインパスワードを入力して例えば、リターンキーを押し下げると自動ログイン部１２が、入力された自動ログインパスワードの照合を行う。
【００６７】
図５に戻り、自動ログインパスワードが適切に照合されると、暗号・復号部３１は、第１の鍵情報９と、第２の鍵情報（自動ログインパスワード）を用いて自動ログイン個人情報１７を復号化し、ＲＡＭ４３に記憶する（ステップ１２１５）。
本実施の形態では、一旦ＲＡＭ４３に記憶した自動ログイン個人情報１７は、自動ログイン部１２の動作を終了するまで保たれるものとする。なお、自動ログインする毎に、自動ログインパスワードをその都度ユーザに入力してもらい、自動ログイン個人情報１７の復号化、及びＲＡＭ４３上の自動ログイン個人情報１７の消去を、その都度行うようにして

セキュリティを高めてもよい。
次に、ログインリクエスト生成部３３がユーザが自動ログインで使用しているサービスサイト用のパラメータ値を自動ログイン個人情報１７で確認し（ステップ１２２０）、自動ログインサイト情報１６と自動ログイン個人情報１７を用いてログインリクエストを生成する。そして、そのログインリクエストをログインリクエスト送信部３４がサーバ５に送信する（ステップ１２２５）。
【００６８】
次に、サーバ５は、クライアント端末３から送信されてきたログインリクエストを受信し、ログイン処理を開始する（ステップ１３０５）。そして、サーバ５は、ユーザのログイン認証がなされると、ログイン認証後の画面データをクライアント端末３に送信する（ステップ１３１０）。
クライアント端末３では、ブラウザ機能部１１がサーバ５から送信されてきたログイン後画面データを用いてログイン後画面を表示する（ステップ１１２０）。
【００６９】
図６（ｄ）は、ログインリクエスト送信部３４がログインリクエストを送信した後、ログイン後画面を表示するまでの間、ブラウザ画面に表示されるログイン中画面の一例を示したものである。ユーザは、ログイン中画面１１３により、現在自動ログインを行っていることを知ることができる。
図６（ｅ）は、ログイン後画面の一例を示した図である。ログイン後画面１１５は、占いサービスを提供するサービスサイトの画面であって、クリックボタン１１６をクリックすると、ユーザの生年月日、星座、名前の画数などによって判断されたユーザの運勢が表示される。
なお、ＲＡＭ４３に記憶した復号後の自動ログイン情報１５は、自動ログイン部１２の動作を終了すると消去されるようになっている。
【００７０】
図７は、既に非接触ＩＣカード７がＩＣカードＲＷ２１にセットされており、自動ログインパスワードも入力され、自動ログインサイト情報１６、自動ログイン個人情報１７の何れもが復号化されている場合のブラウザ１０の動作を説明するためのフローチャートである。これは、例えば、自動ログイン部１２を起動してから２回目以降に自動ログインする場合などが該当する。
図５と重複する部分については説明を簡略化する。
自動ログイン部１２は、自動ログインサイト情報１６を用いてブラウザ機能部１１を監視している（ステップ２２００）。
ユーザがログインページにアクセスすると（ステップ２１００）、サーバ５はログインページをクライアント端末３に送信する（ステップ２３００）。
【００７１】
クライアント端末３では、ログインページを受信すると、ブラウザ監視部３５がＵＲＬをチェックする（ステップ２２０５）。ここでは、このログインページが自動ログインの対象であったとする。
すると、ログインリクエスト生成部３３は、自動ログイン個人情報１７（既にＲＡＭ４３に記憶してある）で、このログインリクエスト情報１４３用のパラメータ値が存在することを確認する（ステップ２２１０）。ここでは、ログインリクエスト情報１４３用のパラメータ値が存在するものとする。
次に、ログインリクエスト生成部３３がログインリクエストを生成し、ログインリクエスト送信部３４がこれをサーバ５に送信する（ステップ２２１５）。
【００７２】
サーバ５では、クライアント端末３からログインリクエストを受信してログイン処理を行い（ステップ２３０５）、ログイン後ページの画面データをクライアント端末３に送信する（ステップ２３１０）。
クライアント端末３は、この画面データを受信し、ブラウザ機能部１１がログイン後ペー

ジを表示する（ステップ２１０５）。

【００７３】

この例では、自動ログインサイト情報１６と、自動ログイン個人情報１７が既に復号化されてＲＡＭ４３に記憶されているため、ユーザが自動ログインパスワードを入力する手間を省略することができる。

そのため、自動ログイン部１２を立ち上げて、２回目以降に自動ログイン対象のサービスサイトにログインする場合は（１回目は、自動ログインパスワードを入力する必要がある）、自動ログインパスワードを入力しないで済む。

【００７４】

図８は、自動ログインサイト情報１６に対応する情報が自動ログイン個人情報１７にない場合に、自動追加部３２が自動ログイン個人情報１７を更新する場合の、ブラウザ１０の動作を説明するための図である。

現在、自動ログイン部１２が起動されていないものとする。

まず、ユーザが非接触ＩＣカード７をＩＣカードＲＷ２１にセットし、自動ログイン部１２を起動する（ステップ３１００）。

すると、暗号・復号部３１が自動ログインサイト情報１６、自動ログイン個人情報１７を復号化すると共に、ブラウザ監視部３５がブラウザ機能部１１の監視を開始する（ステップ３２００）。

【００７５】

ユーザがログインページにアクセスすると（ステップ３１０５）、サーバ５は、ログインページをクライアント端末３に送信する（ステップ３３００）。

次に、ブラウザ監視部３５がこのログインページが自動ログインの対象であることをＵＲＬでチェックし（ステップ３２０５）、ログインページと自動ログイン可能通知を表示する（ステップ３１１０）。

【００７６】

ユーザが自動ログインパスワード入力欄から自動ログインパスワードを入力すると（ステップ３１１５）、自動ログイン部１２は、この自動ログインパスワードを照合し（ステップ３２１０）、暗号・復号部３１が自動ログイン個人情報１７を復号化する（ステップ３２１５）。

次に、ログインリクエスト生成部３３が、このログインページに対応する情報が自動ログイン個人情報１７に存在するか否か確認し、対応する情報が自動ログイン個人情報１７に存在しないことを確認する（ステップ３２２０）。

すると、自動追加部３２がユーザに適当なパラメータ値（ログインＩＤ、パスワードなど）を入力するためのダイアログをブラウザ機能部１１に表示させ（ステップ３２２５）、ユーザがこれに対してパラメータ値を入力する（ステップ３１２０）。

ここで、このダイアログは、サーバ５が送信してきたログインページを用いることもできる。この場合、自動追加部３２は、ユーザがログインページで入力したパラメータ値を取得する。

【００７７】

次に、自動追加部３２は、取得したパラメータ値を用いて自動ログイン個人情報１７を更新する（ステップ３２３０）。

そして、ログインリクエスト生成部３３が更新された自動ログイン個人情報１７を用いてログインリクエストを生成し、ログインリクエスト送信部３４がこのログインリクエストをサーバ５に送信する（ステップ３２３５）。

【００７８】

サーバ５は、クライアント端末３からログインリクエストを受信し、これを用いてログイン処理を行い（ステップ３３０５）、ログイン後ページの画面データをクライアント端末３に送信する（ステップ３３１０）。クライアント端末３では、ブラウザ機能部１１がこのログイン後ページの画面データを用いてログイン後画面を表示する（ステップ３１２５）。

一方、暗号・復号部３１は、更新された自動ログイン個人情報１７を暗号化する（ステップ３２４０）。

【００７９】

図９は、ユーザがＵＲＬ欄に、直接ログインページのＵＲＬを入力した場合の動作を説明するためのフローチャートである。即ち、図５などのフローチャートの例は、サーバ５が送信してきたログインページを受信し、それからこのログインページのＵＲＬが得られるのに対し、図９の例は、ユーザがログインページのＵＲＬをＵＲＬ欄に直接入力したり、アイコン化したログインページをクリックしてＵＲＬ欄にログインページのＵＲＬを入力する場合の例である。

まず、非接触ＩＣカード７をＩＣカードＲＷ２１にセット、自動ログイン部１２を起動する（ステップ４１００）。

次に、暗号・復号部３１が第１の鍵情報９を用いて自動ログインサイト情報１６を復号化すると共に、ブラウザ監視部３５がブラウザ機能部１１の監視を開始する（ステップ４２００）。

【００８０】

ユーザが、ブラウザ画面のＵＲＬ欄にログインページのＵＲＬを入力すると（ステップ４１０５）、ブラウザ監視部３５がこれをチェックする（ステップ４２０５）。そしてブラウザ機能部１１が自動ログイン可能通知を行い（ステップ４１１０）、更に、自動ログインパスワード入力欄を表示する。ユーザが自動ログインパスワードを入力すると（ステップ４１１５）、自動ログイン部１２は、この自動ログインパスワードの照合を行う（ステップ４２１０）。照合が適切に行われると、暗号・復号部３１が自動ログイン個人情報１７を復号化する（ステップ４２１５）。

【００８１】

次に、ログインリクエスト生成部３３が、このログインページに対応する情報が自動ログイン個人情報１７にあることを確認する（ステップ４２２０）。

そして、ログインリクエスト生成部３３がログインリクエストを生成し、ログインリクエスト送信部３４がこれをサーバ５に送信する（ステップ４２２５）。

サーバ５は、このログインリクエストを用いてログイン処理を行い（ステップ４３００）、ログイン後ページの画面データをクライアント端末３に送信する（ステップ４３０５）。

クライアント端末３では、ブラウザ機能部１１が、この画面データを用いてログイン後ページを表示する（ステップ４１２０）。

【００８２】

図１０は、既に、自動ログインサイト情報１６、自動ログイン個人情報１７が復号化されており、ユーザがＵＲＬ欄に直接ログインページのＵＲＬを入力する場合の動作を説明するためのフローチャートである。

まず、ブラウザ監視部３５は、ブラウザ機能部１１を監視している（ステップ５２００）。

次に、ユーザがＵＲＬ欄にログインページのＵＲＬを入力すると（ステップ５１００）、ブラウザ監視部３５がこのＵＲＬが自動ログインサイト情報１６で登録されていることをチェックし（ステップ５２０５）、更にこれに該当する情報が自動ログイン個人情報１７にあることを確認する（ステップ５２１０）。

【００８３】

次に、ログインリクエスト生成部３３がログインリクエストを生成し、ログインリクエスト送信部３４がこのログインリクエストをサーバ５に送信する（ステップ５２１５）。

サーバ５は、このログインリクエストを受信し、ログイン処理を行い（ステップ５３００）、ログイン後ページの画面データをクライアント端末３に送信する（ステップ５３０５）。

クライアント端末３では、ブラウザ機能部１１がこの画面データを用いてログイン後ページを表示する（ステップ５１０５）。

【００８４】
図１１は、自動ログイン情報の他の形態を説明するための図である。この例の自動ログイン情報１５０は、自動ログインサイト情報１６と自動ログイン個人情報１７に区別されておらず、サービス名称、ログインページ情報、ログインリクエスト情報、パラメータが１つの単位としてサービス名称毎に管理されている。
この自動ログイン情報は、例えば、第１の鍵情報９及び第２の鍵情報で復号化可能に暗号化されている。
この場合、ＩＣカードＲＷ２１に非接触ＩＣカード７をセットすると共に、パスワード入力部２２から自動ログインパスワードを入力して自動ログイン情報が復号化され、自動ログイン部１２が動作するようになる。
【００８５】
図１２は、自動ログイン情報の更に他の形態を説明するための図である。
この形態の自動ログイン情報は、自動ログイン情報１６０と、自動ログイン個人情報１６１から構成されている。
ログインを要するサービスサイトは、例えば、銀行預金の管理など秘匿性の高いサイトもあれば、占いサイトのように他者に自動ログイン個人情報が漏れても被害の小さいものまで各種ある。ここでは、自動ログイン個人情報１６１に登録されている情報の重要度をユーザが判断し、重要度の低いものを自動ログイン情報１６０に登録するようにする。
【００８６】
自動ログイン情報１６０は、第１の鍵情報９で復号化可能に暗号化されている。また、自動ログイン個人情報１６１は、第１の鍵情報９、及び第２の鍵情報で復号化可能に暗号化されている。
自動ログイン情報１６０は、サービス名称、ログインページ情報、ログインリクエスト情報、パラメータ値などから構成され、自動ログイン個人情報１６１は、サービス名称、パラメータ値などから構成されている。
そして、自動ログイン情報１６０と自動ログイン個人情報１６１は、サービス名称でひも付けされている。
【００８７】
ユーザは、自動ログイン個人情報１６１に登録されている情報のうち、所望のサービスに関するものだけ、自動ログイン情報１６０に登録することができる。
例えば、図に示した自動ログイン情報１６０では、サービスＡ、Ｂ、Ｅにパラメータ値が登録され、サービスＣ、Ｄには登録されていない。
ログインリクエスト生成部３３は、自動ログイン情報１６０を用いてログインリクエストを生成するように構成されており、パラメータ値が登録されていないものに関しては、ログインリクエストを生成しない。
【００８８】
ユーザは、自動ログインの対象となっているサービスサイトのうち、自動ログイン情報１６０に自動ログイン個人情報１６１に登録してある情報を登録するか否かを判断し、登録してよいと判断した情報を自動ログイン個人情報１６１から自動ログイン情報１６０に登録する。
自動ログイン個人情報１６１は、自動追加部３２によって更新されるが、ユーザは、これを自動ログインに使用するか否かを選択することができる。
【００８９】
なお、本実施の形態では、ＩＣカードＲＷ２１で非接触ＩＣカード７がセットされているか否かを一定時間毎にチェックしているが、これを用いて非接触ＩＣカード７がセットされていない場合にクライアント端末３をロックするように構成することもできる。
このロック機構の形態は各種考えられるが、例えば、非接触ＩＣカード７がＩＣカードＲＷ２１から取り外されている間、ディスプレイのスクリーンセーバを強制的に表示し、更に、キーボードやマウスなどからの入力を受け付けないようにすることができる。そして、クライアント端末３の状態は、非接触ＩＣカード７が取り外された時点の状態に保存さ

れる。
【００９０】
また、あるユーザがクライアント端末３にログインした場合、そのユーザがログアウトするまで、そのユーザの非接触ＩＣカード７でのみロック状態を解除できるように構成することもできる。即ち、クライアント端末３にログインした状態で、そのユーザが非接触ＩＣカード７と共に席を外すなどしてクライアント端末３をロック状態にした場合、他のユーザが自分の非接触ＩＣカード７をセットしてもそのロック状態を解除することはできない。
【００９１】
この場合に、クライアント端末３は、他のユーザからの入力を受け付けない一方、ロック前に行っていた処理をロック中に続行するように構成することもできる。
例えば、数値計算を長時間に渡って行っている場合、クライアント端末３をロック状態にし、外部からの入力は受け付けないが、内部での数値計算は引き続き行うように設定することができる。このように構成することにより、数値計算中に、他のユーザが誤って処理を中断してしまうなどのアクシデントを防止することができる。
【００９２】
また、ＩＣカードＲＷ２１にセットされている非接触ＩＣカード７を検出することにより、クライアント端末３におけるユーザの着席状況を把握することもできる。
例えば、社内にある多数のクライアント端末３のうち、何れのクライアント端末３をどの社員が利用しているかということを管理することができる。
【００９３】
以上に述べた第１の実施の形態により、以下のような効果を得ることができる。
（１）ユーザがネットワーク（インターネット６など）を介してサーバが提供するサービスサイトにログインする際に、そのサービスサイトに対して設定したユーザＩＤ、パスワードを入力することなく、非接触ＩＣカード７などの記憶媒体を用いてログイン情報を読み込むことにより、ログインリクエストの生成、送信を自動化し、利便性、安全性、保守性の優れた自動ログインシステムを提供することができる。
（２）ユーザは、自動ログインシステム１を利用することにより、従来キーボードなどから入力していたユーザＩＤとパスワードを入力する手間を省き、負荷が軽減されるだけでなく、あらゆるインターネット６上のサービスサイトへのログインも自動で行えるなど、利便性の高い自動ログインシステム１を利用できる。
【００９４】
（３）各サービスサイトへのログインには、非接触ＩＣカード７と自動ログインパスワードが必要となり、非接触ＩＣカード７を所持し、かつ、自動ログインパスワードを知るもの以外はログインすることができないため、非接触ＩＣカード７が第三者の手に渡っても悪用されることはない。
（４）キーボードからの入力の負担が軽減されているため、サービスへのログインＩＤやパスワードなどは最大長で複雑なものを使用することができる。そのため、第三者がログインＩＤやパスワードを盗用し、解読して悪用されることが困難となり、セキュリティ性、安全性が高い自動ログインシステム１を利用することができる。
【００９５】
（第２の実施の形態）
図１３は、本発明の第２の実施の形態に係る自動ログインシステム１αの構成を説明するための図である。
第１の実施の形態と同じ構成要素に関しては同じ符合を付すものとし、説明を省略する。また、第１の実施の形態に対応する構成要素には、同じ符合に添え字αを付して示す。
第１の実施の形態では、クライアント端末３は、自動ログインサイト情報１６を自動ログインサイト情報提供サーバ４からダウンロードしたが、本実施の形態では、クライアント端末３でこれを作成する。
【００９６】

クライアント端末３αは、ブラウザ１０αを備えている。ブラウザ１０αは、ブラウザ機能部１１と自動ログイン部１２αから構成されている。
自動ログイン部１２αは、第１の実施の形態の自動ログイン部１２と同様の機能に加え、図示しないが、自動ログインサイト情報１６を生成・更新する自動ログインサイト情報生成部を備えている。
自動ログイン情報１５の構成は第１の実施の形態と同じであるが、本実施の形態の自動ログインサイト情報１６は、自動ログインサイト情報生成部が生成する。
【００９７】
本実施の形態のブラウザ監視部３５は、第１の実施の形態と同様にブラウザ画面のＵＲＬ欄に入力された情報が、ログインページ情報１４２に一致するか監視しているが、一致しなかった場合は、更に自動ログインサイト情報生成部が、この入力された情報がログインページのＵＲＬであるか否かを判断する。この判断は、例えば、「ｌｏｇｉｎ」といったログインページのＵＲＬに使われる頻度の高い文字列が含まれるか否かを判断する。
このように、ＵＲＬ欄に入力された情報で、ログインページ情報１４２に一致せず、「ｌｏｇｉｎ」などの文字列を含む情報は、未登録のログイン情報であると推定される。
【００９８】
自動ログインサイト情報生成部は、ユーザが未登録のログインページにアクセスした場合、ユーザにダイアログを表示してパラメータ値を入力してもらうか、ログインページにユーザが入力した情報を記憶しておくなどして（即ち、どのパラメータにどのようなパラメータ値を入力したか）、これを用いて各種情報を自動ログインサイト情報１６と自動ログイン個人情報１７に登録する。
なお、上の例では、未登録のログインページを自動検出するように設定したが、ユーザが手動で設定するようにしてもよい。即ち、ユーザが未登録のログインページにアクセスした場合、ユーザが自動ログインサイト情報生成部を手動で起動し、自動ログインサイト情報１６、自動ログイン個人情報１７を更新するように構成することもできる。
【００９９】
図１４は、自動ログインサイト情報などを自動更新する場合のブラウザ１０の動作を説明するためのフローチャートである。
まず、非接触ＩＣカード７をＩＣカードＲＷ２１にセットして自動ログイン部１２αを起動する（ステップ６１００）。
そして、暗号・復号部３１が自動ログインサイト情報１６を復号化し、これを用いてブラウザ監視部３５がブラウザ機能部１１の監視を開始する（ステップ６２００）。
【０１００】
次に、ユーザがブラウザ機能部１１からログインページにアクセスする（ステップ６１０５）。ここで、アクセスするログインページは、自動ログインサイト情報１６に登録されていないものであるとする。
次に、サーバ５は、ログインページの画面データをクライアント端末３に送信する（ステップ６３００）。
クライアント端末３はこの画面データを受信し、自動ログインサイト情報生成部が、このログインページが新規（未登録）のものであることを検出する（ステップ６２０５）。
【０１０１】
すると、自動ログインサイト情報生成部は、ブラウザ機能部１１にダイアログを表示させ（ステップ６２１０）、ユーザにパラメータを入力してもらう（ステップ６１１０）。
次に、自動ログイン部１２αは、自動ログインパスワード入力ダイアログをブラウザ機能部１１に表示させ（ステップ６２１５）、ユーザに自動ログインパスワードを入力してもらう（ステップ６１１５）。
自動ログイン部１２αは、自動ログインパスワードの正当性を照合し（ステップ６２２０）、自動ログインパスワードが適当であった場合、暗号・復号部３１が自動ログイン個人情報１７を復号化する。
【０１０２】

次に、ログインリクエスト生成部３３が、ログインページの画面データとユーザが入力したパラメータ値を用いてログインリクエストを生成し、サーバ５に送信する（ステップ６２２５）。
これに対して、サーバ５は、ログイン処理し（ステップ６３０５）、ログイン後ページの画面データをクライアント端末３に送信する（ステップ６３１０）。
クライアント端末３では、ブラウザ機能部１１がこの画面データを用いてログイン後ページを表示する（ステップ６１２０）。
一方、自動ログインサイト情報生成部は、自動ログインサイト情報１６と自動ログイン個人情報１７に、新たに追加された内容を加えて更新し、これを暗号・復号部３１が暗号化する（ステップ６２３０）。
本実施の形態では、クライアント端末３側で自動ログイン情報を更新することができる。
【０１０３】
（第３の実施の形態）
図１５は、第３の実施の形態に係る自動ログインシステム１６のシステム構成の一例を示した図である。
第１の実施の形態と同様な構成要素には同じ符合を付し、説明を省略する。また、第１の実施の形態に対応する構成要素には、同じ符合に添え字ｂを付して示す。
本実施の形態は、インターネット６を介して提供される個々のサービスへのログイン認証を非接触ＩＣカード７ｂからログイン情報を読み込むことにより、自動的にログインするものである。
【０１０４】
本実施の形態では、自動ログイン情報１５ｂを非接触ＩＣカード７ｂに格納する。なお、図示しないが、自動ログインパスワードも暗号化して格納しておく。これは、自動ログイン部１２ｂで復号化し、ユーザがパスワード入力部２２から入力した自動ログインパスワードを照合する際に利用する。
自動ログイン情報１５ｂには、自動ログインサイト情報１６と自動ログイン個人情報１７の両方を記憶させてもよいし、何れか一方を非接触ＩＣカード７ｂに記憶し、他方をクライアント端末３ｂで記憶するように構成してもよい。
【０１０５】
何れか一方を非接触ＩＣカード７ｂに記憶させる場合、自動ログイン個人情報１７を非接触ＩＣカード７ｂに記憶させ、自動ログインサイト情報１６をクライアント端末３ｂで記憶させるようにすると、自動ログイン機能を持つ同様なブラウザ１０を備えた他のクライアント端末３ｂで、非接触ＩＣカード７ｂをセットすることにより、同様に自動ログインを行うことができる。
また、自動ログインサイト情報１６、自動ログイン個人情報１７の双方を非接触ＩＣカード７ｂに記憶させても同様に、他のクライアント端末３ｂから自動ログインすることができる。
第１の実施の形態では、暗号・復号部３１は、記憶装置５５に対してアクセスし、自動ログイン情報１５の復号化、及び暗号化を行ったが、本実施の形態では、暗号・復号部３１は、ＩＣカードＲＷ２１を介して、非接触ＩＣカード７ｂにアクセスし、自動ログイン情報１５ｂの復号化、及び暗号化を行う。
【０１０６】
自動ログイン情報１５ｂは、暗号化したままファイルとしてクライアント端末３ｂのＲＡＭ４３などに書き出すことができるようになっており、自動ログイン部１２ｂは、このファイルを用いて自動ログインすることができる。また、自動ログイン情報１５ｂは非接触ＩＣカード７ｂと共に携帯可能であるため、ユーザは、他のクライアント端末３ｂからも自動ログインすることができる。
このように、本実施の形態では、非接触ＩＣカード７ｂを用いることにより、ブラウザ１０を備えた複数のクライアント端末３ｂからの自動ログインが可能となる。
【０１０７】

また、各サービスサイトへのログインには、非接触ＩＣカード７ｂと自動ログインパスワードが必要となり、非接触ＩＣカード７ｂに格納されているユーザ認証用のパスワード情報を知るもの意外はログインすることができないため、ＩＣカードが第三者の手に渡っても悪用されることはない。
更に、非接触ＩＣカード７ｂを利用可能とするパスワードを設定し、このパスワードを入力しないと、クライアント端末３ｂから自動ログイン情報１５ｂにアクセスできないよう構成すると、更にセキュリティを高めることができる。この場合、クライアント端末３ｂは、ユーザが非接触ＩＣカード７ｂをＩＣカードＲＷ２１にセットしたときに、パスワードを入力するように求めるようにする。
また、このパスワードを自動ログインパスワードとすると、ユーザは１つのパスワードだけ記憶しておけばよく、ユーザの負担を軽減することができる。

【０１０８】

（第４の実施の形態）
図１６は、第４の実施の形態に係る自動ログインシステム１ｃのシステム構成の一例を示した図である。
第１の実施の形態と同様な構成要素には同じ符合を付し、説明を省略する。また、第１の実施の形態に対応する構成要素には、同じ符合に添え字ｃを付して示す。
本実施の形態では、自動ログイン情報を着脱可能な記憶媒体に格納し、ユーザが携帯できるようにする。
第３の実施の形態では、非接触ＩＣカード７ｂが第三者に渡った場合、第１の鍵情報９と自動ログイン情報１５ｂが共にこの第三者に渡ってしまうが、本実施の形態は、自動ログイン情報１５ｃを非接触ＩＣカード７とは別に管理するため、セキュリティが高まる。

【０１０９】

本実施の形態のクライアント端末３ｃは、記憶媒体１９ｃが着脱可能なスロット１８ｃを備えている。スロット１８ｃは、例えば、入出力Ｉ／Ｆ５１（図４）に接続されており、スロット１８ｃにセットされた記憶媒体１９ｃに対してＣＰＵ４１が自由にデータの読み書きを行えるようになっている。
記憶媒体１９ｃは、例えば、不揮発性の半導体メモリであり、この他に、磁気記憶媒体や光ディスクなど、他の形態の記憶媒体を用いることも可能である。

【０１１０】

記憶媒体１９ｃには、自動ログインサイト情報１６と自動ログイン個人情報１７からなる自動ログイン情報１５ｃが記憶されており、暗号・復号部３１は、スロット１９ｃを介して、自動ログイン情報１５ｃを復号化、及び暗号化する。
このため、記憶媒体１９ｃをクライアント端末３ｃと同様な構成を持ったクライアント端末３ｃ'のスロット１８ｃ'にセットすることにより、ユーザはクライアント端末３ｃと同様に自動ログインすることができる。
なお、図示しないが、記憶媒体１９ｃに自動ログインパスワードも暗号化して格納しておく。これは、自動ログイン部１２ｃで復号化し、ユーザがパスワード入力部２２から入力した自動ログインパスワードを照合する際に利用する。

【０１１１】

以上に述べた本実施の形態では、自動ログイン情報１５ｃが自動ログインサイト情報１６と自動ログイン個人情報１７から構成されているとしたが、これに限定するものではなく、例えば、自動ログインサイト情報１６をクライアント端末３ｃに記憶させ、自動ログイン個人情報１７を記憶媒体１９ｃに記憶させるようにしてもよい。
この場合、クライアント端末３ｃ'に自動ログインサイト情報１６を記憶させておけば、記憶媒体１９ｃに記憶された自動ログイン個人情報１７を用いてクライアント端末３ｃ'から自動ログインすることができる。

【０１１２】

本実施の形態では、非接触ＩＣカード７と記憶媒体１９ｃを用いることにより、ブラウザ１０を備えた複数のクライアント端末３ｃからの自動ログインが可能となる。

また、各サービスサイトへのログインには、非接触ＩＣカード７と自動ログインパスワード、及び記憶媒体１９ｃが必要となり、記憶媒体１９ｃに格納されている自動ログインパスワードを知るもの以外はログインすることができないため、非接触ＩＣカード７や記憶媒体１９ｃが第三者の手に渡っても悪用されることはない。

【０１１３】

以上、本発明のいくつかの実施形態について説明したが、本発明は説明した実施形態に限定されるものではなく、各請求項に記載した範囲において各種の変形を行うことが可能である。

例えば、以下のように構成することもできる。

（１）カードを識別する識別番号を保持するカードと、自動ログイン可能な少なくとも１つ以上のサービスサイトに関するログインサイト情報と、前記サービスサイトにログインするための個人情報とを格納する記録媒体と、を用いて複数サイトへログインするクライアント端末において、前記カードの識別番号によって、前記記録媒体から前記ログインサイト情報を読み出すログインサイト情報読み出し手段と、前記個人情報を読み出す際に必要となるパスワードを要求する要求手段と、前記パスワードによって、前記個人情報を読み出す個人情報読み出し手段と、前記ログインサイトに対応する前記個人情報を用いて、自動ログインすることを特徴とするクライアント端末。

（２）カードを識別する識別番号を保持するカードを用いて複数サイトへログインするクライアント端末において、前記カード内に格納される情報を読み出す読み出し手段と、自動ログイン可能な少なくとも１つ以上のサービスサイトに関するログインサイト情報を格納するログインサイト情報記憶手段と、前記サービスサイトへログインするための個人情報を登録する登録手段と、前記個人情報を格納する個人情報記憶手段とを備えるクライアント端末であって、前記カードの識別番号によって、前記ログインサイト情報記憶手段に格納される前記ログインサイト情報を読み出すことを可能とすることを特徴とする。

（３）前記個人情報を読み出す場合には、パスワードを要求する要求手段を更に備えることを特徴とする上記（１）、（２）に記載のクライアント端末。

（４）前記ログインサイト情報には、ログインサイトのＵＲＬが含まれることを特徴とする上記（２）に記載のクライアント端末。

（５）前記要求手段によって得られたパスワードによって、前記ログインサイト情報に対応する個人情報を読み出し、自動的にログインすることを特徴とする上記（３）に記載のクライアント端末。

（６）前記カードは、非接触カードであることを特徴とする上記（２）に記載のクライアント端末。

（７）前記カードを識別する識別番号を保持するカードを用いて複数サイトへログインするログイン方法において、自動ログイン可能な少なくとも１つ以上のサービスサイトに関するログインサイト情報を格納するステップと、前記サービスサイトへログインするための個人情報を登録するステップと、前記個人情報を、対応する前記ログインサイト情報と対応付けて格納するステップと、前記カードの識別番号によって、前記ログインサイト情報を読み出すステップと、前記個人情報を読み出すために、パスワードを要求するステップと、前記個人情報を用いて前記ログインサイトにログインすることを特徴とするログイン方法。

【０１１４】

【発明の効果】

本発明の自動ログインシステムなどによれば、セキュリティ面で安全性を高めることができると共に、各サイトへのログイン操作の負担を軽減することができる。

【図面の簡単な説明】

【図１】本実施の形態のシステム構成を説明するための図である。

【図２】自動ログイン情報の論理的な構成の一例を示した図である。

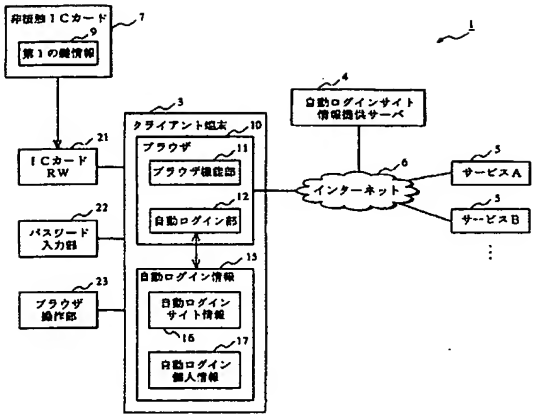
【図３】ブラウザの機能的な構成を説明するための模式図である。

【図４】クライアント端末のハードウェア的な構成の一例を説明するための図である。

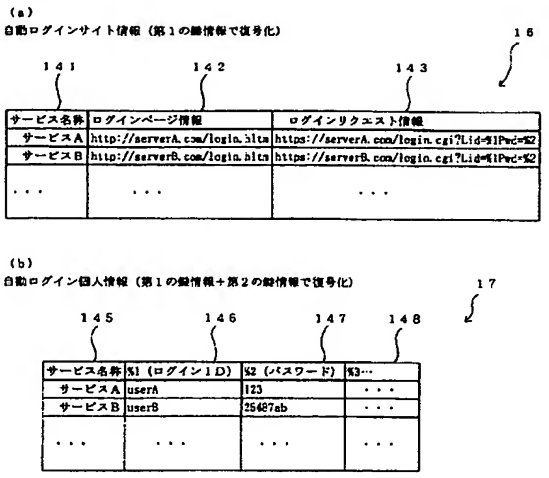
【図５】ブラウザが自動ログインを行う手順を説明するためのフローチャートである。
【図６】自動ログインの際にブラウザ画面に表示される画面の一例を示した図である。
【図７】ブラウザが自動ログインを行う他の手順を説明するためのフローチャートである。
【図８】ブラウザが自動ログインを行う他の手順を説明するためのフローチャートである。
【図９】ブラウザが自動ログインを行う他の手順を説明するためのフローチャートである。
【図１０】ブラウザが自動ログインを行う他の手順を説明するためのフローチャートである。
【図１１】自動ログイン情報の他の形態を説明するための図である。
【図１２】自動ログイン情報の更に他の形態を説明するための図である。
【図１３】本発明の第２の実施の形態に係る自動ログインシステムの構成を説明するための図である。
【図１４】自動ログインサイト情報などを自動更新する場合のブラウザの動作を説明するためのフローチャートである。
【図１５】第３の実施の形態に係る自動ログインシステムのシステム構成の一例を示した図である。
【図１６】第４の実施の形態に係る自動ログインシステムのシステム構成の一例を示した図である。
【図１７】従来例を説明するための図である。
【符号の説明】

１　自動ログインシステム	３　クライアント端末
５　サーバ	６　インターネット
７　非接触ＩＣカード	９　第１の鍵情報
１０　ブラウザ	１１　ブラウザ機能部
１２　自動ログイン部	１５　自動ログイン情報
１６　自動ログインサイト情報	１７　自動ログイン個人情報
２１　ＩＣカードＲＷ	２２　パスワード入力部
２３　ブラウザ操作部	３１　暗号・復号部
３２　自動追加部	３３　ログインリクエスト生成部
３４　ログインリクエスト送信部	３５　ブラウザ監視部
４１　ＣＰＵ	４２　ＲＯＭ
４３　ＲＡＭ	４５　表示手段
４６　入力手段	４７　出力手段
４８　通信制御手段	５２　記憶媒体駆動装置
５５　記憶装置	５６　ブラウザプログラム
５７　自動ログインサイト情報データベース	
５８　自動ログイン個人情報データベース	

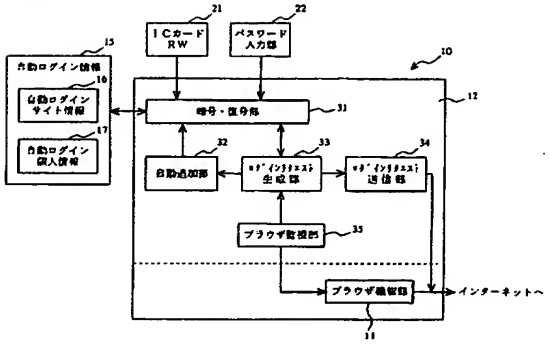
【図１】


1
非接触ICカード
7
第１の鍵情報
9
3
クライアント端末
10
ブラウザ
11
ブラウザ機能部
12
自動ログイン部
13
自動ログイン情報
自動ログイン
サイト情報
16
自動ログイン
個人情報
17
ICカード
RW
21
パスワード
入力部
22
ブラウザ
操作部
23
4
自動ログインサイト
情報提供サーバ
6
インターネット
5
サービスA
サービスB

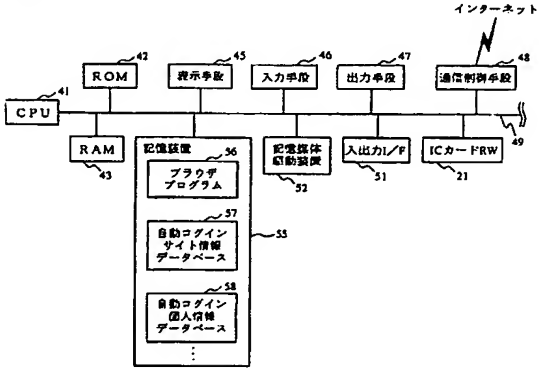
【図２】


(a)
自動ログインサイト情報（第１の鍵情報で復号化）
16
141
142
143
サービス名称
ログインページ情報
ログインリクエスト情報
サービスA
http://serverA.com/login.htm
https://serverA.com/login.cgi?Lid=%1Pwd=%2
サービスB
http://serverB.com/login.htm
https://serverB.com/login.cgi?Lid=%1Pwd=%2
(b)
自動ログイン個人情報（第１の鍵情報＋第２の鍵情報で復号化）
17
145
146
147
148
サービス名称
%1（ログインID）
%2（パスワード）
%3…
サービスA
userA
123
サービスB
userB
25487ab

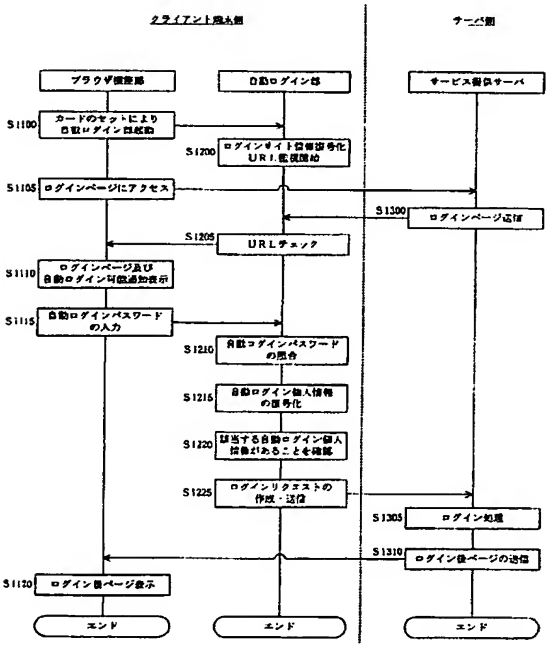
【図３】


21
ICカード
RW
22
パスワード
入力部
13
自動ログイン情報
16
自動ログイン
サイト情報
17
自動ログイン
個人情報
10
12
暗号・復号部
31
32
自動通知部
33
ログインリクエスト
生成部
34
ログインリクエスト
送信部
35
ブラウザ監視部
ブラウザ機能部
インターネットへ
11

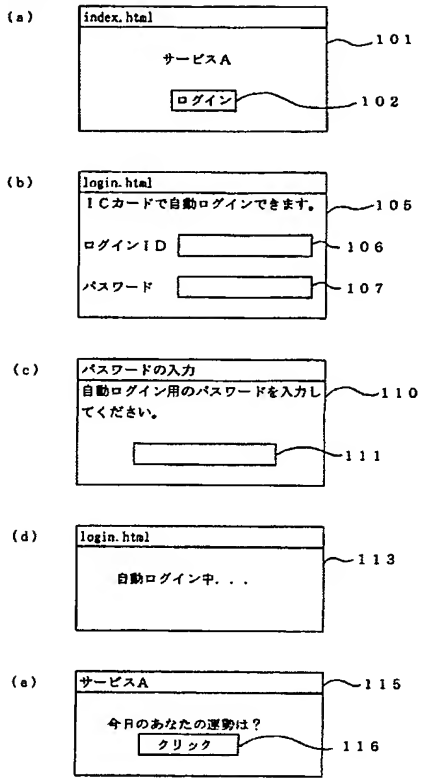
【図４】


インターネット
42
ROM
45
提示手段
46
入力手段
47
出力手段
48
通信制御手段
41
CPU
49
RAM
43
記憶装置
56
ブラウザ
プログラム
57
自動ログイン
サイト情報
データベース
55
58
自動ログイン
個人情報
データベース
記憶媒体
駆動装置
52
入出力I/F
51
ICカードRW
21

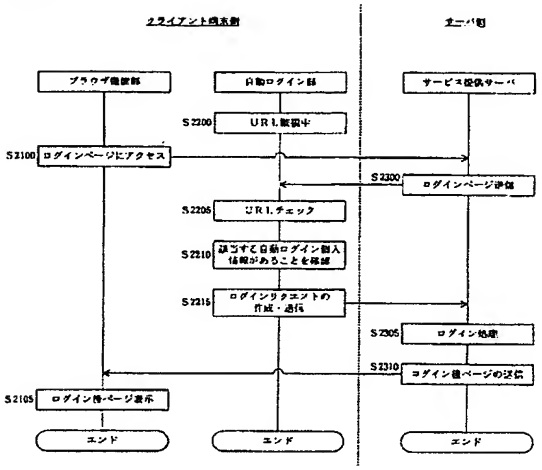
【図５】


クライアント端末側
サーバ側
ブラウザ機能部
自動ログイン部
サービス提供サーバ
S1100
カードのセットにより
自動ログイン起動
S1200
ログインサイト情報復号化
URL監視開始
S1105
ログインページにアクセス
S1300
ログインページ送信
S1205
URLチェック
S1110
ログインページ及び
自動ログイン可能通知表示
S1115
自動ログインパスワード
の入力
S1210
自動ログインパスワード
の照合
S1215
自動ログイン個人情報
の復号化
S1220
該当する自動ログイン個人
情報があることを確認
S1225
ログインリクエストの
作成・送信
S1305
ログイン処理
S1310
ログイン後ページの送信
S1120
ログイン後ページ表示
エンド
エンド
エンド

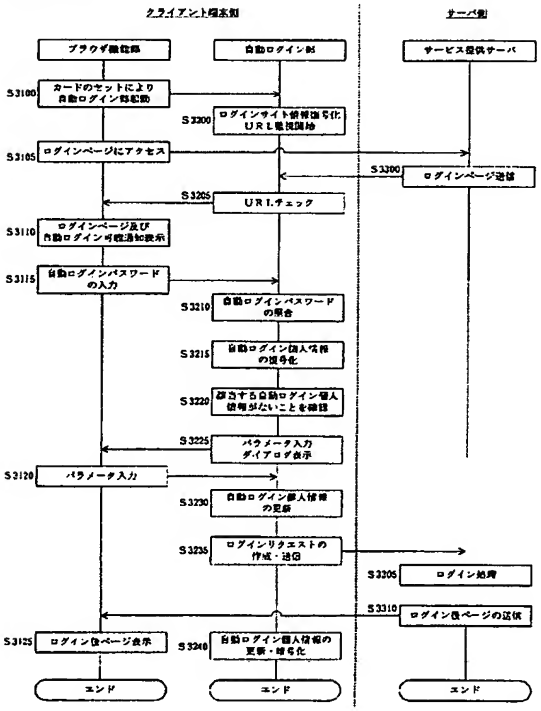
【図６】


(a)
index.html
サービスA
ログイン
101
102
(b)
login.html
ＩＣカードで自動ログインできます。
ログインＩＤ
パスワード
105
106
107
(c)
パスワードの入力
自動ログイン用のパスワードを入力してください。
110
111
(d)
login.html
自動ログイン中．．．
113
(e)
サービスA
今日のあなたの運勢は？
クリック
115
116

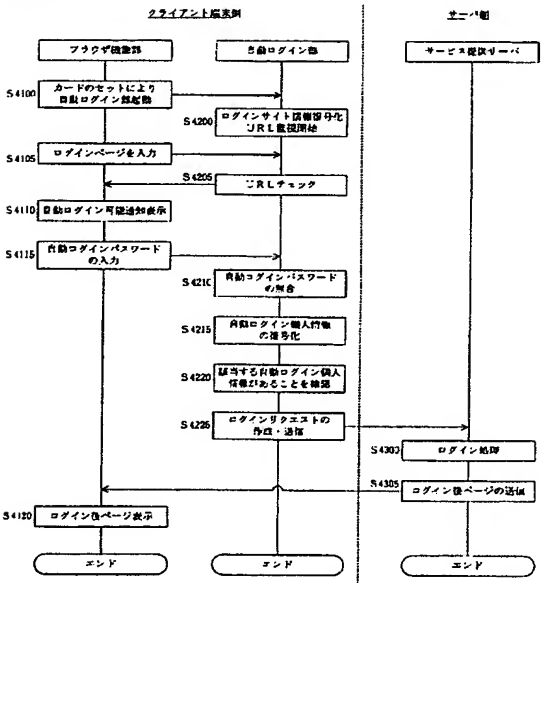
【図７】


クライアント端末側
サーバ側
ブラウザ機能部
自動ログイン部
サービス提供サーバ
S2200 URL監視中
S2100 ログインページにアクセス
S2300 ログインページ送信
S2205 URLチェック
S2210 該当する自動ログイン個人情報があることを確認
S2215 ログインリクエストの作成・送信
S2305 ログイン処理
S2310 ログイン後ページの送信
S2105 ログイン後ページ表示
エンド
エンド
エンド

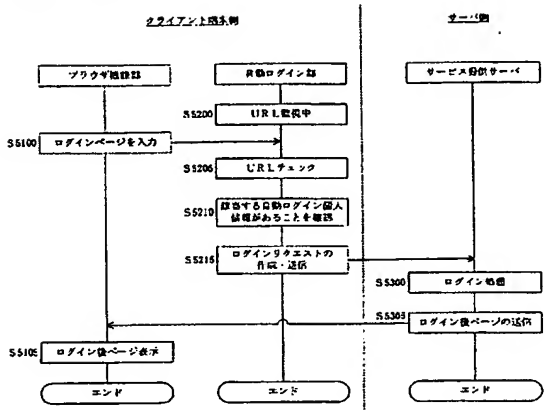
【図８】


クライアント端末側
サーバ側
ブラウザ機能部
自動ログイン部
サービス提供サーバ
S3100 カードのセットにより自動ログイン部起動
S3200 ログインサイト情報暗号化 URL監視開始
S3105 ログインページにアクセス
S3300 ログインページ送信
S3205 URLチェック
S3110 ログインページ及び自動ログイン可能通知表示
S3115 自動ログインパスワードの入力
S3210 自動ログインパスワードの照合
S3215 自動ログイン個人情報の復号化
S3220 該当する自動ログイン個人情報があることを確認
S3225 パラメータ入力ダイアログ表示
S3120 パラメータ入力
S3230 自動ログイン個人情報の更新
S3235 ログインリクエストの作成・送信
S3305 ログイン処理
S3310 ログイン後ページの送信
S3125 ログイン後ページ表示
S3240 自動ログイン個人情報の更新・暗号化
エンド
エンド
エンド

【図９】


クライアント端末側
サーバ側
ブラウザ機能部
自動ログイン部
サービス提供サーバ
S4100 カードのセットにより自動ログイン部起動
S4200 ログインサイト情報暗号化 URL監視開始
S4105 ログインページを入力
S4205 URLチェック
S4110 自動ログイン可能通知表示
S4115 自動ログインパスワードの入力
S4210 自動ログインパスワードの照合
S4215 自動ログイン個人情報の復号化
S4220 該当する自動ログイン個人情報があることを確認
S4225 ログインリクエストの作成・送信
S4305 ログイン処理
S4310 ログイン後ページの送信
S4120 ログイン後ページ表示
エンド
エンド
エンド

【図１０】



【図１１】

自動ログイン情報（第１の鍵情報＋第２の鍵情報で復号化）

160

サービス名称	ログインページ情報	ﾛｸﾞｲﾝﾘｸｴｽﾄ情報	%1(ﾛｸﾞｲﾝID)	%2(ﾊﾟｽﾜｰﾄﾞ)	%3･･
サービスA	http://serverA･･･	https://serverA･･･	userA	123	･･･
サービスB	http://serverB･･･	https://serverB･･･	userB	25487ab	･･･
･･･	･･･	･･･	･･･	･･･	･･･

【図１２】

（a）

自動ログイン情報（第１の鍵情報で復号化）

160

サービス名称	ログインページ情報	ﾛｸﾞｲﾝﾘｸｴｽﾄ情報	%1(ﾛｸﾞｲﾝID)	%2(ﾊﾟｽﾜｰﾄﾞ)	%3･･･
サービスA	http://serverA･･･	https://serverA･･･	userA	123	･･･
サービスB	http://serverB･･･	https://serverB･･･	userB	25487ab	･･･
サービスC	http://serverC･･･	https://serverC･･･			
サービスD	http://serverD･･･	https://serverD･･･			
サービスE	http://serverE･･･	https://serverE･･･	userE	ab123cd	
･･･	･･･	･･･	･･･	･･･	･･･

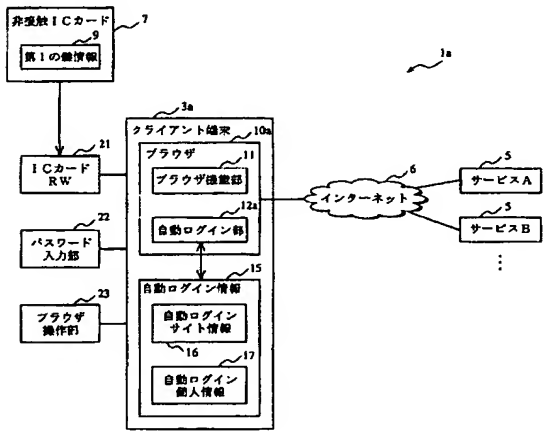
（b）

自動ログイン個人情報（第１の鍵情報＋第２の鍵情報２で復号化）

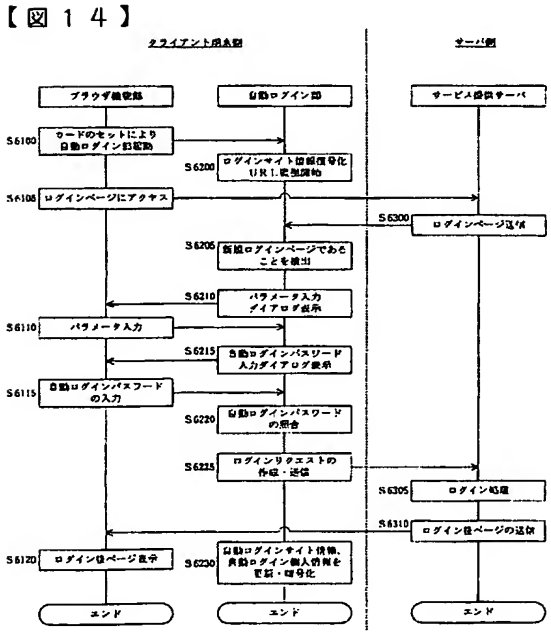
161

サービス名称	%1（ログインＩＤ）	%2（パスワード）	%3･･･
サービスA	userA	123	･･･
サービスB	userB	25487ab	･･･
サービスC	userC	efg456	･･･
サービスD	userD	dhtchsekc1s58e	･･･
サービスE	userE	ab123cd	･･･
･･･	･･･	･･･	･･･

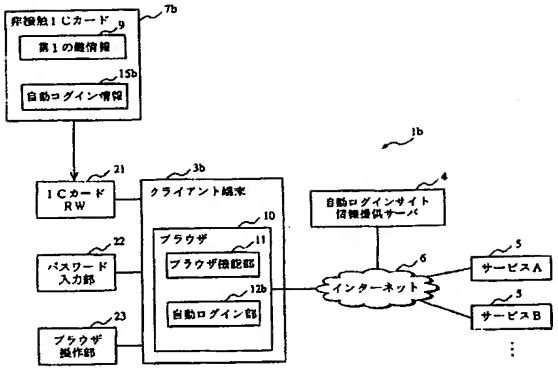
【図１３】



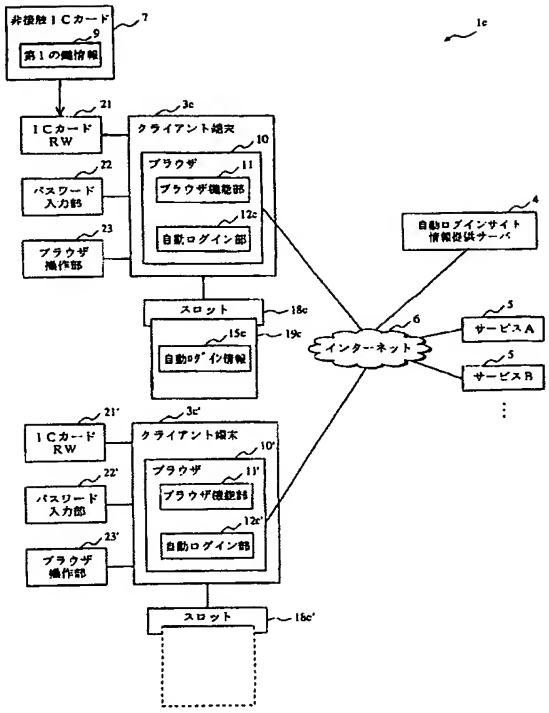
【図１４】



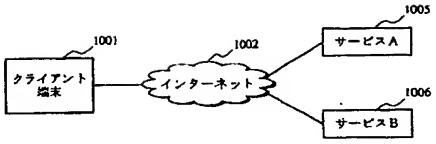
【図１５】


非接触ＩＣカード
7b
第１の識情報
9
自動ログイン情報
15b
ＩＣカード RW
21
クライアント端末
3b
ブラウザ
10
ブラウザ機能部
11
自動ログイン部
12b
パスワード 入力部
22
ブラウザ 操作部
23
1b
自動ログインサイト 情報提供サーバ
4
インターネット
6
サービスＡ
5
サービスＢ
5

【図１６】


非接触ＩＣカード
7
第１の識情報
9
1c
ＩＣカード RW
21
クライアント端末
3c
ブラウザ
10
ブラウザ機能部
11
自動ログイン部
12c
パスワード 入力部
22
ブラウザ 操作部
23
スロット
18c
自動ログイン情報
15c
19c
自動ログインサイト 情報提供サーバ
4
インターネット
6
サービスＡ
5
サービスＢ
5
ＩＣカード RW
21'
クライアント端末
3c'
ブラウザ
10'
ブラウザ機能部
11'
自動ログイン部
12c'
パスワード 入力部
22'
ブラウザ 操作部
23'
スロット
18c'

【図１７】


クライアント 端末
1001
インターネット
1002
サービスＡ
1005
サービスＢ
1006

フロントページの続き

(51)Int.Cl.[7]	FI			テーマコード（参考）
	H04L	9/00	673E	
	H04L	9/00	675Z	

(72)発明者 中山 浩
東京都品川区北品川6丁目7番35号 ソニー株式会社内
(72)発明者 長島 敦
東京都品川区北品川6丁目7番35号 ソニー株式会社内

Fターム(参考) 5B085 AE01 AE08 AE13
5J104 AA07 EA03 NA05 NA38